PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-174797

(43)Date of publication of application : 23.06.2000

(51)Int.Cl. H04L 12/46

H04L 12/28

G11B 20/10

H04L 9/32

H04L 12/66

H04L 29/06

(21)Application number : 11-209836

(22)Date of filing : 23.07.1999

(71)Applicant : TOSHIBA CORP

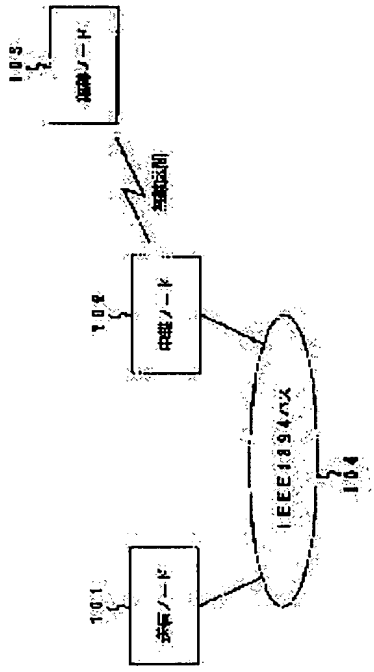
(72)Inventor : SAITO TAKESHI

TAKAHATA YOSHIAKI

(30)Priority

Priority number : 10292824 Priority date : 30.09.1998 Priority country : JP

(54) REPEATER AND COMMUNICATION EQUIPMENT



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a repeater capable of a contents protection procedure between equipment not connected to the same network.

SOLUTION: This repeater is connected to a first network 104 and a second network and is provided with a function for presenting the equipment 103 on the second network to the side of the first network 104 as the one on the present repeater 102, the function for transmitting a corresponding control command to the equipment 103 in the case of receiving the control command addressed to the equipment 103 from the equipment 101 on the first network 104, the function for transmitting contents protection information to the equipment 103 without changing it in the case of receiving it addressed to the equipment 103 from the equipment 101 and the function for transmitting contents to the equipment 103 without changing them in the case of receiving the contents protected by a contents key obtained from the previous contents protection information from the equipment 101 to the equipment 103.

LEGAL STATUS

[Date of request for examination] 03.12.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3583657

[Date of registration] 06.08.2004

[Number of appeal against examiner's

decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the communication device which communicates through networks, such as the repeating installation and the IEEE1394 bus from which the data transfer between networks, such as an IEEE1394 bus and a wireless network, is relayed, and a wireless network.
[0002]
[Description of the Prior Art] In recent years, the so-called "digitization of the home AV environment" attracts big attention for initiation of digital broadcasting, sale of a digital AV equipment, etc. Also as the possibility of various compression, and multimedia data, digital AV data have the possibility of processing, and the outstanding description, like there is no degradation, even if it reproduces how many times, and it is thought that the application will spread increasingly from now on.
[0003] However, on the other hand, there is also a side face "contents can be copied illegally easily" in this digital AV technique. That is, since the duplicate which original quality moreover crosses eternally by "the copy of a bit", and does not have degradation theoretically about any digital contents can be made, the so-called problem of an "illegal copy" occurs.
[0004] Some techniques for preventing this "illegal copy" are examined. One of them is "the 1394CP contents protection-system specification (1394CP Content Protection System Specification)" currently examined by CPTWG (copy protection technical workgroup). This technique is a technique of preventing from reading contents, except both who performed authentication procedure beforehand between transceiver nodes, enabled it to share a cryptographic key (contents key), enciphered and transmitted the contents to transmit henceforth, and performed authentication procedure between the nodes connected to the IEEE1394 bus about the contents (for example, MPEG data etc.)

to transmit. Since the value of a contents key does not understand the node which omits authentication procedure by doing in this way, even if it is able to incorporate the data (data enciphered) transmitted, it cannot decrypt this code. The node which can participate in such authentication is what is considered only as the node which the certificate authority set beforehand permitted, and it becomes possible to prevent that an inaccurate node receives a cryptographic key and to prevent an illegal copy beforehand.

[0005]

[Problem(s) to be Solved by the Invention] Also at the minimum rate, it is a network system with the description which was very excellent to have the QOS transfer facility equipped with automatic configuration recognizing ability in 100Mbps(es) and the network itself etc., and, so, the IEEE1394 bus has built the status of a de facto standard as a network for digital one AV for homes.

[0006] However, IEEE1394 has induced constraint various "when connecting other networks with IEEE1394" to because of that of these descriptions. For example, since the approach these networks extend not having the rapidity of 100 or more Mbpses generally and the automatic configuration recognizing ability of IEEE1394 as it is to these networks cannot take easily when connecting an IEEE1394 bus with a wireless network or a public network, the approach of extending an IEEE1394 protocol to wireless or a public network as it is cannot be used. then, the protocol conversion gateway is arranged between IEEE1394 and other networks, such as a wireless network and a public network, and the approach of interconnecting, the approach of the so-called substitute server which also obtains one of the two's screen oversize service, and is offered as service of one of the two's network, etc. are proposed.

[0007] When it is going to apply these approaches to 1394 copy protection stated by the Prior art, it is in the situation that this copy protection technique is defined only about the IEEE1394 bus in the present condition. The present condition is that there is no technique for extending this copy protection technique "when connecting other networks with IEEE1394."

[0008] This invention was made in consideration of the above-mentioned situation, and aims at offering extensible repeating installation and an extensible communication device also on the other networks which interconnected the copy protection technique not only with IEEE1394 but with this.

[0009] Moreover, this invention aims at offering the repeating installation and the communication device which enable contents protection procedure between the equipment which is not connected in the same network.

[0010]

[Means for Solving the Problem] 1st interface means by which the repeating installation concerning this invention (claim 1) was connected to the 1st network, The 2nd interface means connected to the 2nd network, and a substitute configuration means to indicate the equipment on said 2nd network, service, or a subunit to said 1st network side as a thing on self-repeating installation, A control command receiving means to receive this equipment, service, or the control command signal addressed to a subunit from said 1st network side, A control command transmitting means to transmit the signal corresponding to said control command signal received with this control command receiving means to the equipment on said 2nd network, service, or a subunit, A contents protection information receiving means to receive said equipment, the service, or the contents protection information addressed to a subunit disclosed with said substitute configuration means from the equipment on said 1st network, Modification is not added to the contents protection information received with this contents protection information receiving means, but it is characterized by providing a contents protection information transfer means to transmit to the equipment on said 2nd network, service, or a subunit.

[0011] 1st interface means by which the repeating installation concerning this invention (claim 2) was connected to the 1st network, A substitute configuration means to indicate respectively the equipment on the 2nd interface means connected to the 2nd network, and the 1st and 2nd networks, service, or a subunit to the network side of another side as a thing on self-repeating installation, A control command receiving means to receive this equipment, service, or the control command signal addressed to a subunit from the network side indicated with said substitute configuration means, A control command transmitting means to transmit the signal corresponding to said control command signal received with this control command receiving means to the equipment on the network indicated with said substitute configuration means, and a different network, service, or a subunit, A contents protection information receiving means to receive said equipment, the service, or the contents protection information addressed to a subunit disclosed with said substitute configuration means from the equipment on said 1st or 2nd network, A contents protection information transfer means not to add modification to the contents protection information received with this contents protection information receiving means, but to transmit to the equipment on the network of said another side, service, or a subunit, It is said equipment, the service, or addressing to a subunit indicated with said substitute configuration means from the equipment on said 1st or 2nd network. A contents receiving means to receive the contents protected with

the contents key obtained from said contents protection information, Modification is not added to said contents which received with this contents receiving means, but it is characterized by providing a contents transfer means to transmit to the equipment on the network of said another side, service, or a subunit.

[0012] desirable -- said contents protection information -- the authentication between the equipment on said 1st network, service or a subunit, and the equipment on said 2nd network, service or a subunit -- and -- or you may make it be the information about the procedure of the contents protection including key exchange

[0013] "According to this invention, it is the pair which is performing the transmission or reception of contents which should be protected, for example. The equipment, the service, or the subunit on the 2nd network which the substitute configuration means offers It sets between "the equipment on the 1st network" as ". (Equipment, service, or a subunit is hereafter called equipment etc.) The partner of contents protection procedure recognizing it as "the equipment on the 1st network", or "the equipment on the 2nd network which the substitute configuration means offers etc. being" the repeating installation concerned to the last Since contents protection procedure can be performed, it becomes unnecessary to take into consideration about another network "the equipment on the 2nd network which the substitute configuration means offers etc. is connected in" through repeating installation. ["the equipment on the 1st network" or] Moreover, when repeating installation relays the procedure in fact, without changing contents, the contents protection procedure can be directly performed between "the equipment on the 2nd network which the substitute configuration means offers etc. and equipment". ["the equipment on the 1st network"]

[0014] Moreover, according to this invention, the contents which should be protected can be sent into a receiving side, without changing the protection format, and contents can be sent into an end end in the protected form.

[0015] 1st interface means by which the repeating installation concerning this invention (claim 4) was connected to the 1st network, A substitute configuration means to indicate respectively the equipment on the 2nd interface means connected to the 2nd network, and the 1st and 2nd networks, service, or a subunit to the network side of another side as a thing on self-repeating installation, A control command receiving means to receive this equipment, service, or the control command signal addressed to a subunit from the network side indicated with said substitute configuration means, A control command transmitting means to transmit the signal corresponding to said control command signal received with this control command receiving means to the equipment on the network indicated with said substitute configuration means, and a different network,

service, or a subunit, Between self-repeating installation with the equipment on said 1st network, service, or a subunit Between self-repeating installation with the 1st contents safeguard which takes the necessary procedure for contents protection, and the equipment on said 2nd network, service or a subunit From the equipment on the 2nd contents safeguard which takes the necessary procedure for contents protection, and said network of either the 1st or a 2nd A contents receiving means to be the equipment on the self-repeating installation indicated with said substitute configuration means, service, or addressing to a subunit, and to receive the contents enciphered based on said contents safeguard of either the 1st or a 2nd, The contents which received with said contents receiving means are enciphered based on the contents safeguard of said 1st or 2nd any or another side. It is characterized by providing a contents transmitting means to transmit to the equipment on the network of said 1st or 2nd any or another side, service, or a subunit.

[0016] In between the "equipment" which are the pair which is performing the transmission or reception of contents which should be protected, for example according to this invention [the equipment on the 2nd network etc. and "the equipment on the 1st network"] Since the partner of contents protection procedure can perform contents protection procedure, recognizing it as "the equipment on the 1st network", or "the equipment on the 2nd network etc. being" the repeating installation concerned to the last, It becomes unnecessary to take into consideration about another network "the equipment on the 2nd network etc. is connected in" through repeating installation. ["the equipment on the 1st network", or] Moreover, for example, repeating installation will perform contents protection procedure after all by carrying out termination of the contents protection procedure, respectively, respectively between "the equipment on the 2nd network, etc. and repeating installation", and between repeating installation and "the equipment on the 1st network", and can protect contents at an end end after all.

[0017] Moreover, the data transmitted in all the paths between the equipment on the 2nd network etc. from the equipment on the 1st network will be enciphered, and it becomes possible to prevent an illegal copy etc.

[0018] You may make it the cipher system used by said 1st contents safeguard and said 2nd contents safeguard preferably based on key information which is a different method or is different.

[0019] Preferably, the closure of said contents receiving means and said contents transmitting means may be made to be carried out to the same LSI. By this, since the contents data which are not enciphered flow, it carries out that a probe is applied separately etc. between this decryption means and an encryption means, it intercepts

contents data from here, and becomes possible [preventing beforehand] about committing an illegal copy.

[0020] Preferably, it may be made to make 1st key information used in the procedure of said contents protection in said 1st contents safeguard, and 2nd key information used in the procedure of said contents protection in said 2nd contents safeguard into the same thing. By this, the information (a key, seed, etc.) about the key of the encryption data transmitted to the network of another side told from one network by transmitting to the network of another side as it is With the equipment on the network of another side, since playback of this encryption key is attained, the code decode function and re-encryption function between a contents receiving means and a contents transmitting means become unnecessary, and it becomes possible to attain reduction of the large cost of repeating installation, and improvement in the speed of processing speed.

[0021] Moreover, you may make it refuse the Request to Send of data to be enciphered from the equipment by the side of the network of another side, and the equipment of the others on the network of another side when the enciphered data transfer is being performed preferably. If it does in this way, it will become possible to prevent beforehand enciphered data transfer which is different in the network side of another side.

[0022] desirable -- either [said] the 1st or the 2nd -- it may be made to perform procedure of said contents protection in the contents safeguard of another side per a contents unit, a service unit, or subunit using predetermined key information. When it becomes possible to transmit the enciphered data to coincidence since two or more cryptographic keys can be defined and two or more encryption data are transmitted from the equipment on one network between the equipment by the side of the network of another side by this, the management to the case where two or more equipments are on one network etc. is attained.

[0023] You may make it provide further preferably a configuration information receiving means to receive the configuration information containing the existence of an authentication format (device certification) of this equipment from the equipment on said 1st and 2nd networks, service, or a subunit, and a configuration recognition means to perform this equipment, service, or configuration recognition of a subunit based on each configuration information which received with said configuration information receiving means. By this, the substitute service which a substitute configuration means constitutes can be automatically constituted now, it has it, and implementation by the plug and play of a procedure which results in contents protection procedure is attained.

[0024] Moreover, in case said substitute configuration means transmits data to the

equipment of said 1st network, you may make it notify preferably the equipment, the service, or the subunit which transmits these data in which self-repeating installation has carried out the substitute configuration to the equipment of this 1st network beforehand. It becomes possible to notify where an authentication demand should be given by this to the equipment on the 1st network which received this notice.

[0025] 1st interface means by which the repeating installation concerning this invention (claim 10) was connected to the 1st network, Between self-repeating installation with the 2nd interface means connected to the 2nd network, and the equipment on said 1st network, service or a subunit Between self-repeating installation with the 1st contents safeguard which takes the necessary procedure for contents protection, and the equipment on said 2nd network, service or a subunit From the equipment on the 2nd contents safeguard which takes the necessary procedure for contents protection, and said network of either the 1st or a 2nd A contents receiving means to be the equipment on self-repeating installation, service, or addressing to a subunit, and to receive the contents enciphered based on said contents safeguard of either the 1st or a 2nd, The contents which received with said contents receiving means are enciphered based on the contents safeguard of said 1st or 2nd any or another side. A contents transmitting means to transmit to the equipment on the network of said 1st or 2nd any or another side, service, or a subunit is provided. It is characterized by making into the same thing 1st key information used in the procedure of said contents protection in said 1st contents safeguard, and 2nd key information used in the procedure of said contents protection in said 2nd contents safeguard.

[0026] The communication device concerning this invention (claim 11) between the interface means connected to the network, and other equipments on said network, service or a subunit at least -- authentication procedure -- and -- or with a copy protection processing means to perform predetermined contents protection procedure including key exchange procedure The enciphered contents which gave the address of a self-communication device to other equipments on said network An identifiable identifier is further given to a meaning for the address and these contents of a self-communication device through a network virtual channel top. From a contents transmitting means to transmit, and other equipments on said network A receiving means to receive the inquiry about the service or the subunit which gave said identifier through said virtual channel top, and has transmitted said enciphered contents, or a plug, It is characterized by answering this inquiry and providing the notice means which gives the notice about the corresponding service, a subunit, or a plug to other equipments on said network.

[0027] The communication device concerning this invention (claim 12) between the interface means connected to the network, and other equipments on said network, service or a subunit at least -- authentication procedure -- and -- or with a copy protection processing means to perform predetermined contents protection procedure including key exchange procedure From other equipments on said network, the enciphered contents to which the address of other equipments on this network was given In the form where these contents were given to the identifiable identifier by the meaning, other equipments on this network through a network virtual channel top As opposed to a contents receiving means to receive, and other equipments on said network A transmitting means to transmit the inquiry about the service or the subunit which gave said identifier through said virtual channel, and has transmitted said enciphered contents, or a plug, It is characterized by providing a receiving means to receive the notice about the service applicable to said inquiry, a subunit, or a plug from other equipments on said network.

[0028] It becomes possible to specify the subunit or plug of transmission of the encryption data transmitted by the specific virtual channel, or each reception according to this invention. By subsequent authentication and key exchange Since it becomes possible to show clearly "To want to perform authentication and key exchange about the data transmitted or received from this subunit (or plug)", and it has and the same nodes can define two or more keys as coincidence, An exchange of two or more encryption data is attained. It becomes possible to specify the subunit or plug of transmission of the encryption data transmitted with the specific identifier, or each reception according to this invention. Or by subsequent authentication and key exchange Since it becomes possible to show clearly "To want to perform authentication and key exchange about the data transmitted or received from this subunit (or plug)", and it has and the same nodes can define two or more keys as coincidence, An exchange of two or more encryption data is attained.

[0029] An interface means by which the communication device concerning this invention (claim 13) was connected to the network, the enciphered contents to other equipments on said network with a contents transfer means to transmit or receive through the flow of the transmitting address, a transmit port, the receiving address, and a receive port constructed, come out of and identified The logical port appointed beforehand is used among other equipments on said network. at least -- authentication procedure -- and -- or when a copy protection processing means to perform predetermined contents protection procedure including key exchange procedure is provided and it performs said predetermined contents protection procedure, it is

characterized by performing this in the unit of said flow.

[0030] You may make it give the identifier of said flow to the information which sets for the procedure of at least a part included in said predetermined contents protection procedure, and is preferably made it.

[0031] Since it becomes possible to show "To want to perform authentication and key exchange about this flow" clearly, and it has by subsequent authentication and key exchange, in order to be able to perform the definition of a different key for every flow according to this invention, and the same nodes can define two or more keys as coincidence, an exchange of two or more encryption data is attained.

[0032] The communication device concerning this invention (claim 15) between the interface means connected to the network, and other equipments on said network, service or a subunit at least -- authentication procedure -- and -- or with a copy protection processing means to perform predetermined contents protection procedure including key exchange procedure The enciphered contents to which the address of the equipment of a transmitting side was given to other equipments on said network In the form to which the identifiable identifier was given by the meaning, the equipment of this transmitting side these contents through a network virtual channel top To the information which sets for the procedure of at least a part which possesses a contents transceiver means to transmit or receive, and is included in said predetermined contents protection procedure, and is made it It is characterized by the service and the subunit which exchange said enciphered contents, a virtual channel, the identifier of a plug, or the equipment of said transmitting side giving at least one of identifiable identifiers to a meaning for said contents.

[0033] Since according to this invention it becomes possible to show clearly "To want to perform authentication and key exchange about the data transmitted or received from this subunit, the plug, or the virtual channel", and it has and the same nodes can define two or more keys as coincidence by authentication and key exchange, an exchange of two or more encryption data is attained. Or since according to this invention it becomes possible to show clearly "To want to have this subunit or a plug to said specific identifier, and to perform authentication and key exchange about the data transmitted or received", and it has and the same nodes can define two or more keys as coincidence by authentication and key exchange, an exchange of two or more encryption data is attained.

[0034] 1st interface means by which the repeating installation concerning this invention (claim 16) was connected to the 1st network, The 2nd interface means connected to the 2nd network, and the equipment, the service or the subunit on the 1st network, at least

-- authentication procedure -- and -- or with the copy protection processing means of predetermined contents protection procedure ****** 1 including key exchange procedure The equipment, the service, or the subunit on the 2nd network, at least -- authentication procedure -- and -- or with the copy protection processing means of the predetermined contents protection procedure 2nd including key exchange procedure A contents receiving means to receive the data containing the specific contents enciphered from said 1st interface means, A decryption means to decrypt said enciphered data which were received from said 1st interface means with the key for contents protection for which it is provided with said 1st copy protection processing means, A conversion means to change said decrypted data into the data of another coding format, It is characterized by providing an encryption means to encipher said decrypted data with the key for contents protection for which it is provided with said 2nd copy protection processing means, and a contents transmitting means to transmit said enciphered data to said 2nd interface means.

[0035] Like [according to this invention / it is the contents from which the data to which the 1st network is made to transmit should be protected, and / in case the communication bands of the 1st network and the 2nd network differ remarkably] Changing data format with a conversion means, when transmitting to the 2nd network in a different data format from the original data is called for It becomes possible to encipher the data transmitted in all the paths between the equipment on the 2nd network etc., and to prevent an illegal copy etc. from the equipment on the 1st network also in both the sections (both data format).

[0036] Preferably, in repeating installation according to claim 16, while indicating the equipment on said 2nd network, service, or a subunit to said 1st network side as a thing on self-repeating installation When the information addressed to the equipment indicated as a thing on self-repeating installation, service, or a subunit is received from the equipment by the side of said 1st network While transmitting the information on the contents according to this information to the equipment on said 2nd network, service, or a subunit As a thing on self-repeating installation, while indicating the equipment on said 1st network, service, or a subunit to said 2nd network side When the information addressed to the equipment indicated as a thing on self-repeating installation, service, or a subunit is received from the equipment by the side of said 2nd network A substitute configuration means to transmit the information on the contents according to this information to the equipment on said 1st network, service, or a subunit is provided further. Said substitute configuration means The equipment on one [said] 1st or 2nd network, the equipment on the network of said 1st or 2nd another side,

service, or a subunit, at least -- authentication procedure -- and -- or, in performing predetermined contents protection procedure including key exchange procedure While performing the equipment on one [said] network, and this predetermined contents protection procedure using one [said] 1st or 2nd copy protection processing means It may be made to perform the equipment on the network of said another side, service or a subunit, and this predetermined contents protection procedure using the copy protection processing means of said 1st or 2nd another side.

[0037] In between the "equipment" which are the pair which is performing the transmission or reception of contents which should be protected according to this invention [the equipment on the network of another side etc. and "the equipment on one network"] Since the partner of contents protection procedure can perform contents protection procedure, recognizing it as "the equipment on one network", or "the equipment on the network of another side etc. being" the repeating installation concerned to the last, It becomes unnecessary to take into consideration about another network "the equipment on the network of another side etc. is connected in" through repeating installation. ["the equipment on one network", or] Moreover, in fact, repeating installation will perform contents protection procedure after all by carrying out termination of the contents protection procedure, respectively between "the equipment on the network of another side etc. and repeating installation" and repeating installation, and "the equipment on one network", and can protect contents at an end end after all.

[0038] It sets to repeating installation according to claim 16 preferably. Moreover, said contents receiving means Said 2nd copy protection processing means is used. The equipment, the service, or the subunit on said 2nd network, When at least a part is performed among said predetermined contents protection procedure and it is completed normally It may be made to perform at least a part using said 1st copy protection processing means among the equipment of said 1st network, service or a subunit, and said predetermined contents protection procedure. In addition, at least a part is for example, authentication procedure among said predetermined contents protection procedure. When doing in this way, and the equipment on the 2nd network, service, or a subunit can know now beforehand whether it is the device which is sufficient for reliance, performs the equipment etc. and the authentication procedure on the 2nd network first and fails in authentication with the equipment on the 1st network etc. after that, it becomes saving of the part which does not need to perform authentication with the equipment on the 1st network etc. anew, a communication resource, or process resources.

[0039] Moreover, a processor means for the communication device concerning this invention to include the program for screen drawing with which control of the 1st equipment is presented and to receive the 1st control program and to work this, A screen creation means to create the panel screen which constitutes at least the part of the screens which this processor means draws, A storage means to memorize the correspondence relation between the command to said panel screen, and the command for control of said 1st equipment, A subunit processing means to open to the 2nd equipment by making said panel screen into a subunit, When the command to said subunit is received, it is characterized by having changed this command into the command for control of said 1st equipment with reference to said storage means, and providing a means to send this out. Generally, the appliance control which let the panel screen pass to being called a virtual machine and preparing a count environment in order to work the above control programs should just prepare the easy count environment in order just to prepare an easy command form. According to this invention, it becomes possible also to the 2nd equipment without said control program to offer the control interface of said 1st equipment in the form of a panel screen.

[0040] In addition, this invention concerning equipment is materialized also as invention concerning an approach, and this invention concerning an approach is materialized also as invention concerning equipment.

[0041] Moreover, this invention concerning equipment or an approach is materialized also as a record medium which recorded the program (or in order to realize the function which is equivalent to the invention concerned at a computer in order to operate a computer as a means equivalent to the invention concerned) for performing the procedure equivalent to the invention concerned on the computer and in which computer read is possible.

[0042]

[Embodiment of the Invention] Hereafter, the gestalt of implementation of invention is explained, referring to a drawing.

[0043] (1st operation gestalt) Drawing 1 is an example of the whole configuration of the home network of a certain home.

[0044] Three, the transmitting node 101, the junction node 102, and the wireless node 103, are connected to this home network, the transmitting node 101 and the junction node 102 are connected to the IEEE1394 bus (cable) 104, and the junction node 102 and the wireless node 103 are connected to the wireless network, respectively. However, the communication link of each node has become possible mutually by approach which is mentioned later.

[0045] With this operation gestalt, the MPEG image sent out from the transmitting node 101 is relayed by the junction node 102, and the case where it transmits to the wireless node 103 via the wireless section is explained as an example. The MPEG image data transmitted between the transmitting node 101 and the wireless node 103 for protection of copyrights (prevention of an illegal copy) in that case consider the case where it is enciphered.

[0046] In addition, in drawing 1 , although three nodes are shown, of course, the node other than these may be connected (also in other operation gestalten mentioned later, it is the same).

[0047] An example of the internal structure of the transmitting node 101 is shown in drawing 2 .

[0048] The transmitting node 101 is equipment which is storing MPEG image data in the interior, and sends out MPEG image data through the IEEE1394 bus 104 according to a demand. In order to prevent beforehand carrying out an illegal copy on an IEEE1394 bus in that case, in being required, it has the function which enciphers and sends out the MPEG image data to send out. Therefore, it also has a device for exchanging authentication data, a cryptographic key, etc. for the node which receives MPEG image data.

[0049] As shown in drawing 2 , this transmitting node 101 It lets the IEEE1394 interface 401, the AV/C protocol processing section 402 which performs processing of an AV/C protocol, the copy protection processing section 403 which performs processing about the copy protection in an AV/C protocol, and IEEE1394 pass. A cryptographic key K is got from the ISO signal sender and receiver 404 which transmits and receives a synchronous channel among the data transmitted and received about the data which let it pass and are carried out, the MPEG storage section 406 which is the storage of an MPEG image, and the copy protection processing section 403. It has the encryption section 405 which enciphers an MPEG image and is sent out to the ISO signal sender and receiver 404. Here, the copy protection processing section 403 has the format Acert for authentication.

[0050] Next, an example of the internal structure of the junction node 102 is shown in drawing 3 .

[0051] The junction node 102 besides the function which acts to a wireless section side as the forward of the data (MPEG image data) received from the IEEE1394 bus side It becomes the substitute server of a wireless node to the node by the side of an IEEE1394 bus. It becomes the substitute server of the node by the side of an IEEE1394 bus (this operation gestalt transmitting node 101) to the node by the side of the function to offer

the function of a wireless node in a substitute, and the wireless section, and the function to offer the function of the node by the side of an IEEE1394 bus in a substitute exists.

[0052] As shown in drawing 3 , this junction node 102 The configuration information of the node on the IEEE1394 interface 201, the wireless interface 202, the AV/C protocol processing section 203, the ISO signal sender and receiver 204, the wireless ISO signal sender and receiver 205 that transmit and receive the signal of the synchronous channel by the side of the wireless section, and an IEEE1394 bus Collect or As opposed to the 1394 bus-arrangement recognition section 206 side with the function which advertises its configuration information (information about what kind of function he has etc.) on IEEE1394, and an IEEE1394 bus side exhibit the node by the side of the wireless section, and service (subunit) in a substitute, or The node by the side of the wireless section, the command to service, etc. are received in a substitute, and the need is accepted in this at a wireless section side. Carry out protocol conversion, and send out or or collect the configuration information of the node on the substitute subunit configuration section 207 which performs substitute public presentation of the node/service by the side of IEEE1394 (subunit), substitute reception / translation of a command, etc. to a wireless section side, and the wireless section, or Processing about the wireless section configuration recognition section 209 and copy protection with the function which advertises its configuration information (information about what kind of function he has etc.) on the wireless section is performed. It is related with the copy protection processing which straddles 1394 buses and the wireless section. It has the copy protection control / forward section 210 to which it acts as the forward of the information exchanged transparent, and the wireless node control packet transceiver section 211 which transmit and receive the control packet exchanged in the wireless section.

[0053] Next, an example of the internal structure of the wireless node 103 is shown in drawing 4 .

[0054] There is not necessarily no need that the so-called IEEE1394 protocols (a physical-layer protocol, link layer protocol, etc.) are working in the wireless section, and although IEEE802.11, wireless LAN, etc. assume using the wireless protocol of arbitration, especially with this operation gestalt, it assumes that it is a wireless network with the so-called QOS function (synchronous transmission function). However, this operation gestalt will not be restricted if a wireless section part is asked for a QOS function.

[0055] In order that the wireless node 103 which is not the so-called IEEE1394 node may communicate with the node (this operation gestalt transmitting node 101)

connected with the IEEE1394 bus, the junction node 102 has emulated the node and function (subunit) on an IEEE1394 bus as mentioned above. That is, it sees from the wireless node 103 and the junction node 102 serves as a node by the side of the so-called IEEE1394 bus, and a substitute server of a function. Although the wireless node 103 communicates by considering these (the node and function by the side of IEEE1394) to be the functions of the junction node 102, it changes in fact by the protocol conversion which needs the junction node 102, and data putting.

[0056] As shown in drawing 4 , this wireless node 103 has the code decryption section 305 which decrypts this using the contents key K to which the wireless interface 301, the wireless node control packet transceiver section 302, the copy protection processing section 303, the wireless ISO signal sender and receiver 304, and the enciphered streams (MPEG image etc.) that received are passed from the copy protection processing section 303, the MPEG decoding section 306, and the display section 307 which displays an image.

[0057] As the copy protection processing section 303 of the wireless node 103 is mentioned later, it has the authentication format Bcert and the issue engine of the authentication is the same issue engine as the issue engine of the authentication format Acert of the transmitting node 101 (image sending-out subunit).

[0058] Next, the sequence of the whole MPEG image after performing actual copy protection is explained, referring to drawing 5 / drawing 6 (the whole example of a sequence), drawing 7 / drawing 8 (example of a flow chart of the transmitting node 101), drawing 9 / drawing 10 / drawing 11 (example of a flow chart of the junction node 102), and drawing 12 / drawing 13 (example of a flow chart of the wireless node 103).

[0059] First, the wireless node 103 notifies its configuration information to the junction node 102 (step S501). This notice prepares IEEE1212 register in a wireless node, and may be performed in the form where its configuration information is described here. Configuration information is a it's (wireless node's) having MPEG decoding / display function, having the authentication format for authentication and key exchange, etc. Here, this authentication format may notify to coincidence that it is the format which the specific copy protection engine defined, or may notify the purport which is the authentication format for the copy protection for IEEE1394 to coincidence.

[0060] Here, authentication is explained briefly.

[0061] When transmitting the contents (data) which should take copyrights, such as a movie and a TV program, into consideration for a network top, those contents should protect in the code. When intercepted on a network during these data transfers, it is because an illegal copy becomes possible. As a cure to this, the data encryption to

transmit is effective.

[0062] Next, becoming a problem is the problem "whether there is any risk of having sent data to the doubtful thing." Even if it enciphered and sent data, when the node (it has the key which solves a code) of the sent point has malice even if, data should not be sent in a too decipherable form (when it is thought that you will copy illegally). The cure to this is authentication. That is, before passing the key which solves this code to a receiving side, a receiving side is the structure which takes the check of being what does not commit injustice (the key which solves a code is passed only to the receiving-side node which was able to take the check).

[0063] Specifically, the certificate authority gives the data called "an authentication format" beforehand to both the node of a transmitting side, and the node of a receiving side to the node (or subunit) recognized as "This node (or subunit) does not work unjustly." that node (or subunit) can trust having this "authentication format" in the right form -- ** (injustice is not committed) -- it can think. Then, in advance of the above-mentioned data transfer, an authentication format is exchanged between transceiver nodes (or subunit), when an authentication format is able to be checked in a right form, it restricts, and the key (or data which become the origin for generating a key) for solving a code is notified, and how to transmit a network top for the data enciphered with the key is taken.

[0064] Now, such an authentication format is beforehand given to the wireless node 103 by the certificate authority, and it has "the right which receives / reproduces encryption data in a just form." Here, the authentication format which the wireless node 103 has is set to "Bcert."

[0065] In case the wireless node 103 notifies its configuration information at step S501 of drawing 5 , he may add having the authentication format to this configuration information (step S801). For example, like drawing 14 , this wireless node 103 has MPEG decoding / display function in configuration information, and this function's having an authentication format further and its authentication format have what which issue engine published, and the information on **.

[0066] In addition, if it considers as the approach the junction node 102 recognizes the configuration of the wireless node 103, the approach transmit the packet which the junction node 102 asks that a configuration is to the wireless node 103, and the wireless node 103 replies to this etc. is possible.

[0067] Now, the junction node 102 which received this configuration information checks that the wireless node 103 has an authentication format or having MPEG decoding / display function (step S701).

[0068] The junction node 102 advertises this MPEG decoding / display function to an IEEE1394 bus side as a subunit of junction node 102 self, in order that the wireless node 103 may tell having MPEG decoding / display function to the node by the side of an IEEE1394 bus (step S502). The purport "he has MPEG decoding / display function" in IEEE1212 register is indicated, or when an AV/C protocol receives an inquiry of a subunit configuration, specifically, a response is returned in the form where he has MPEG decoding / display subunit (the node connected to IEEE1394 will recognize it as this function existing in the junction node 102 by this).

[0069] Therefore, the junction node 102 has the substitute table 208 in the substitute subunit configuration section 207. The substitute table 208 is a table which matching with the form which the junction node 102 is advertising in the substitute, and its stereo is describing like drawing 15 / drawing 16 .

[0070] Here, the substitute advertisement of the MPEG decoding / display function of the wireless node 103 is carried out as an own subunit of a junction node like drawing 15 (steps S702 and S703).

[0071] For this reason, the structure of the junction node 102 seen from the transmitting node 101 will look like drawing 17 (step S601).

[0072] Although the above was explanation about an IEEE1394 bus side, the same relation as this is realized also at the wireless section. That is, the junction node 102 investigates the device by the side of an IEEE1394 bus, service, a subunit configuration, etc., and is offering these substitute services to the wireless section side. Therefore, a setup like drawing 16 is made and the structure of the junction node 102 seen from the wireless node looks like drawing 18 .

[0073] Now, the transmitting node 101 recognized that MPEG decoding / display subunit is in the junction node 102 For the purpose of transmitting an MPEG image to this subunit a 1394 bus top -- synchronous channel #x -- being established -- an AV/C protocol -- "-- with this synchronous channel #x (plug to receive (for example, plug in AV/C specified by 1394TAs)) MPEG decoding / display subunit is connected and the instruction with display an image" is issued (steps S503 and S602). Since the transmitting node 101 is interpreting it as that to which this subunit hits the junction node 101, the transmission place of an instruction is the junction node 102.

[0074] The junction node 102 which received this (step S704) interprets the instruction packet which received, recognizes that that instruction is an instruction to MPEG decoding / display subunit to which oneself is offering substitute service, and recognizes that the stereo of this instruction place is in the wireless node 103 with reference to the substitute table 208 (step S705).

[0075] Therefore, the data received through synchronous channel #x of an IEEE1394 bus The synchronous channel (#y) of the wireless section is secured that it should act to a wireless node side as a forward (step S706). Furthermore, the ISO signal sender and receiver 204 (synchronous channel #x are received) and the wireless ISO signal sender and receiver 205 (synchronous channel #y is transmitted) are connected. It can be made to carry out at the wireless section the forward of the input data (ISO data) inputted from 1394 interfaces 201 (steps S504 and S707).

[0076] Furthermore, the instruction with "since data are transmitted through wireless synchronous channel #y, receive this, input into an MPEG decoder and display the result on a display" is transmitted in the form of a wireless node control packet to the wireless node 103 (steps S505 and S708).

[0077] An example of this wireless node control packet is shown in drawing 19 .

[0078] As shown in drawing 19 , they are the contents to which it urges transmitting and displaying the data (MPEG image) transmitted to the wireless node 103 through wireless synchronous channel #y on MPEG decoding / display function. Moreover, the information about the subunit (the image transmitting function of the junction node 102; in fact, if it has that function in the substitute of the transmitting node 101, it will advertise) which transmits this data (MPEG image) into this is also notified collectively.

[0079] The wireless node 103 which received this recognizes that data are sent through wireless synchronous channel #y (step S802). The wireless node 103 recognizes it as the transmitting origin of this data being the image transmitting subunit of the junction node 102 (as mentioned above, actual data transmitting origin is the transmitting node 101). For this reason, the information "the transmitting origin of the data transmitted through this wireless synchronous channel is the image transmitting subunit of the junction node 102" may be included in this wireless node control packet.

[0080] Then, the transmitting node 101 lets synchronous channel #x pass, and transmits the enciphered MPEG image (steps S603 and S506). The junction node 102 which received this acts as the forward of this at the wireless section, as set up previously (steps S709 and S507).

[0081] Although the junction node 102 can recognize that this is encryption data when it receives the MPEG image enciphered at step S506, it recognizes as it being necessary to transmit to a wireless network side, and acts as the forward of this as it is. The purport which needs the procedure of authentication and key exchange may be memorized later.

[0082] Thus, the enciphered MPEG image reaches the wireless node 103 (step S803). The node ID of the junction node 102 may be contained in this MPEG image as a source address. For this reason, although it can recognize the wireless node 103 that this

MPEG image reaches from the junction node 102, since the wireless node 103 does not have the key K for solving this code at this time (or it does not have data which become the origin for generating that key), it cannot solve a code in this condition and cannot take out an MPEG image. Here, it recognizes that authentication procedure is as required for the wireless node 103 as the transmitting origin of an MPEG image.

[0083] Then, the wireless node 103 (copy protection processing section 303) transmits an authentication demand to the transmitting origin of encryption data. As stated previously, the transmitting origin of the above-mentioned encryption data is recognized to be the junction node 102 (an inner subunit classification = image transmitting subunit and subunit of subunit ID=b (referred to as b= 0)) by the wireless node 103.

[0084] Moreover, like S521 of drawing 5 , in "wireless node, subunit classification =MPEG decoding / display subunit has received wireless synchronous channel #y to the junction node 102, and it is the subunit of subunit ID=c (referred to as c= 0). Which subunit has transmitted encryption data to wireless synchronous channel #y? An inquiry of the implications " may be transmitted. On the other hand, the junction node 102 returns answerback with "subunit ID=0 of an image transmitting subunit has transmitted to wireless synchronous channel #y" (steps S522, S731, and S831). Thereby, the wireless node 103 can recognize that the point which attests is the image transmitting subunit of a junction node.

[0085] Thus, the destination of an authentication demand is recognized and an authentication demand is transmitted to the junction node 102 (subunit ID=0 of an inner image transmitting subunit). As the method of this transmission, it may be good also considering the destination of an authentication demand packet as "an image transmitting subunit (subunit ID=0) of a junction node", the information of "an image transmitting subunit (subunit ID=0)" may be put into the location of the arbitration of an authentication demand packet, and you may indicate that it says that an authentication demand place is an image transmitting subunit (subunit ID=0) clearly. In the case of the former, it means that the procedure of authentication and key exchange is included in each subunit of a junction node. In the case of the latter, it means that the processing section of specification with a junction node bundles up, and performs authentication and key exchange of each subunit.

[0086] The authentication format Bcert of the wireless node 103 is given to an authentication demand in that case (steps S804 and S508). Bcert may be an authentication format of MPEG decoding / display subunit of the wireless node 103. In addition, the copy protection processing section may prepare an authentication format for every subunit (every subunit classification) and every subunit ID.

[0087] The junction node which received the authentication demand (step S710) recognizes that the demand place of this authentication demand is the transmitting node 101 (subunit ID=a of an image transmitting subunit (referred to as a= 0)) in fact with reference to the substitute table 208.

[0088] It is subunit ID=0 of MPEG decoding / display subunit that the junction node 102 has received synchronous channel #x in "junction node to the transmitting node 101. Which subunit of a transmitting node has transmitted encryption data to synchronous channel #x? An inquiry of the implications " may be transmitted (steps S523, S631, and S732). On the other hand, the transmitting node 101 returns answerback with "subunit ID=0 of an image transmitting subunit has transmitted to synchronous channel #x" (steps S524, S631, and S732).

[0089] Thus, if the partner of an authentication demand is recognized, it will act as the forward of the authentication demand which received at step S508 to the transmitting node 101, without changing contents (leaving Bcert etc. as it is) (steps S509 and S711). That is, a junction node can transmit a destination address, the authentication format of those other than the subunit which is the destination of an authentication demand, etc. transparent.

[0090] In the case of a transfer of an authentication demand, as explained previously, it may be good also considering the destination of an authentication demand packet as an image transmitting subunit (subunit ID=0), and the information which specifies the subunit concerned may be put into the location of the arbitration of an authentication demand packet, and you may indicate that it says that an authentication demand place is the subunit concerned clearly.

[0091] This authentication demand will reach the transmitting node 101 in a form as it is by acting as a forward, without changing the contents of the authentication demand here. After all between the transmitting node 101 and the wireless node 103 It is possible to perform the above procedure, without an actual authentication procedure's progressing, beginning the junction node 102 moreover, and information, such as a value of the key which becomes clear as a result of the authentication, being known by other nodes.

[0092] The transmitting node 101 which received the authentication demand is interpreted as it being the authentication demand to which this has been sent from MPEG decoding / display subunit of the junction node 102 (step S604). Then, ID (Bdid) which can specify MPEG decoding / display subunit of the wireless node 103 tends to be extracted from Bcert (step S605), and it is going to give the same authentication demand to the transmitting origin of an authentication demand with this too. However,

the transmitting node 101 is not that Bcert is an authentication format of the wireless node 103 conscious, and if it is an authentication format of the junction node 102 (MPEG decoding / display subunit) rather, it is conscious.

[0093] The authentication formats Acert and Bdid of the transmitting node 101 (image sending-out subunit) are included in this authentication demand. Here, since the transmitting node 101 is interpreting the transmitting origin of this authentication demand (step S509) as it being the junction node 102 (MPEG decoding / display subunit), the transmission place of this authentication demand serves as the junction node 102 too (steps S606 and S510).

[0094] With reference to the substitute table 208, the junction node 102 which received this (step S712) recognizes that the original demand place of this authentication procedure is the wireless node 103 (MPEG decoding / display function), and acts as the forward of this authentication procedure demand to the wireless node 103, without changing contents (leaving Acert etc. as it is) (steps S511 and S713). The transmitting origin of this authentication demand is the junction node 102.

[0095] The wireless node 103 which received this is interpreted as it being the authentication demand to which this has been sent from the image transmitting subunit of the junction node 102 (step S805). Then, ID (Adid) which can specify the image subunit of the transmitting node 101 tends to be extracted from Acert, and it is going to perform the remaining procedure required for exchange of an authentication key to the transmitting origin of an authentication demand. In addition, also in this case, the wireless node 103 is not that Acert is an authentication format of the transmitting node 101 conscious, and is that it is an authentication format of the junction node 102 (image transmitting subunit) rather conscious.

[0096] As a remaining procedure required for exchange of this authentication key, the wireless node 103 transmits authentication and a key exchange procedure packet to the transmitting origin (node which the wireless node is interpreting) of an authentication demand (step S512). The device ID (Adid) of key exchange initial value, a signature, and the transmitting node (image transmitting subunit) contained in Acert etc. is contained in this authentication and key exchange procedure packet (step S806). Here, since the wireless node 103 is interpreting the transmitting origin of this authentication demand (step S511) as it being the junction node 102 (image transmitting subunit), the transmission place of this authentication demand serves as the junction node 102 too.

[0097] With reference to the substitute table 208, the junction node 102 which received this recognizes that the original demand place of this authentication procedure is the transmitting node 101 (image transmitting subunit), and acts as the forward of this

authentication procedure packet to the transmitting node 101, without changing contents (steps S513 and S714). The transmitting origin of this packet is the junction node 102.

[0098] The same procedure as this is performed also to the direction of the transmitting node 101 -> junction node 102 -> wireless node 103 (steps S514, S515, S609, S715, and S807).

[0099] The transmitting node 101 and the wireless node 103 which received this authentication procedure packet perform the check of Tampa of whether the packet which received is altered, respectively, the check of whether the authentication format sent by the partner is a right thing, etc., and draw the common authentication key Kauth using the given value. This common authentication key Kauth is a key which it has in common between a transmitting node (image transmitting subunit) and a wireless node (MPEG decoding / display function), and it comes to be able to perform sharing this key Kauth, without being known by others other than these both (the transmitting node 101, wireless node 103) at this time (step S607, steps S608 and S808).

[0100] It comes to be able to perform count of the contents key K which actually enciphers an MPEG stream using this authentication key Kauth. Although a concrete procedure is skipped here, you may come to be able to perform count of the contents key K by sending an exchange key and seed's (seed) value to the wireless node 102 separately like the copy protection method (5C methods) of IEEE1394 from the transmitting node 101 (steps S518 and S519).

[0101] Now, it does in this way and the value of the contents key K can be shared now between the transmitting node 101 (image transmitting subunit) and the wireless node 103 (MPEG decoding / display function).

[0102] Here, the transmitting node 101 enciphers the MPEG image to transmit in the encryption section 405 using the contents key K (step S610), and transmits this to the junction node 102 (MPEG decoding / display subunit) through synchronous channel #x of 1394 buses (steps S516 and S611).

[0103] The junction node 102 lets the wireless ISO signal sender and receiver 205 pass from the ISO signal sender and receiver 204, and transmits the enciphered MPEG image which is sent through synchronous channel #x from the transmitting node 101 to wireless synchronous channel #y (steps S517 and S716).

[0104] The wireless node 103 which received this decrypts the value of an MPEG image using the value of Key K (step S809, step S810). The decrypted MPEG data are decrypted in the MPEG decoding section 306 (step S811), and indicate this by playback in the display section 307 (step S812).

[0105] Thus, also in the environment of interconnect where a substitute node exists between 1394 buses and a wireless network, the nodes (at this operation gestalt, they are the transmitting node 101 and the wireless node 103) of · end can perform authentication procedure and key exchange procedure, and it has become the structure in which other nodes including the junction node 102 cannot know the contents further. Moreover, the required data transfer of contents protection, such as an actual MPEG image, is also enciphered in all the paths as it cannot copy, and safe data transfer is possible. It becomes possible to perform data transfer which took copy protection into consideration also in the environment of such interconnect by this.

[0106] In addition, although the above operation gestalt has performed authentication procedure, exchange procedure of a cryptographic key, etc. per subunit of a node, it can also perform this per wireless node. In addition, what is necessary is just to apply this, for example, since the 2nd following operation gestalt explains the example performed per node.

[0107] Moreover, although procedure for authentication and key exchange has been performed after reception of encryption data, of course, the above operation gestalt is available, even if it performs this procedure in advance of encryption data reception. For example, this procedure may be performed at the time of starting of equipment and applicable application.

[0108] (2nd operation gestalt) Next, the 2nd operation gestalt is explained.

[0109] With the 1st operation gestalt, the transmitting node and the wireless node have performed authentication procedure and key exchange procedure directly and mutually. That is, directly, the transmitting node (image subunit) and the wireless node (MPEG decoding / display function) attested each other, performed exchange procedure of a cryptographic key, and have exchanged encryption data. Under the present circumstances, although the junction node achieved the redundancy of MPEG decoding / display function of a wireless node to the transmitting node and came the redundancy of the image transmitting subunit of a transmitting node sure enough to the wireless node, it was a form carried out to a function about the above-mentioned authentication procedure and the part of an exchange of encryption data in the subunit which was acting for the mere forward of these data.

[0110] On the other hand, the 2nd operation gestalt shows the example in the case of carrying out termination of the exchange, a series of copy protection procedure, i.e., authentication procedure, of encryption data in a junction node. That is, each copy protection procedure is closed between a transmitting node and a junction node and between the junction node and the wireless node. That is, also in this operation gestalt,

a junction node is an example in the case of carrying out termination of the responsibility about an MPEG data encryption transfer of the wireless section while the junction node itself has an authentication format and the junction node itself carries out termination of the responsibility about an MPEG data encryption transfer of the 1394 bus sections about copy protection, although substitute service is offered to a transmitting node or a wireless node.

[0111] An example of the whole configuration of the home network of a certain home is shown in drawing 20 . This whole configuration is the same as that of the 1st operation gestalt fundamentally.

[0112] An example of the internal structure of the transmitting node 2101 is shown in drawing 21 . The same is fundamentally [as the 1st operation gestalt] said of this.

[0113] Next, an example of the internal structure of the junction node 2102 is shown in drawing 22 .

[0114] Like the 1st operation gestalt, the junction node 2102 serves as a substitute server of a wireless node to the node by the side of an IEEE1394 bus, serves as a substitute server of the node by the side of an IEEE1394 bus (this operation gestalt transmitting node 2101) to the node by the side of the function to offer the function of a wireless node in a substitute, and the wireless section, and has the function offer the function of the node by the side of an IEEE1394 bus in a substitute.

[0115] Although it has the function which acts to a wireless section side as the forward of the data (MPEG image data) received from the IEEE1394 bus side, moreover, the point which is different from the 1st operation gestalt The procedure about copy protection authentication data, encryption, etc. about both the IEEE1394 bus section and the wireless section Termination is carried out in this junction node 2102. About an IEEE1394 bus side, the authentication format Bcert in the IEEE1394 copy protection processing section 2208 About a wireless section side, it has the authentication format Ccert in the wireless section copy protection processing section 2212, respectively. About the encryption data inputted from the synchronous channel of 1394 buses It is the point which steps on the process of transmission for the MPEG image decrypted [which were decrypted and was code-decrypted] in the receiving -> code decryption section 2204 in the ISO signal receive section 2203 on a wireless synchronizing signal in the encryption section 2205 in the re-encryption -> wireless ISO signal sender and receiver 2206.

[0116] These authentication formats may also be at a time as one for every IEEE1394 interface and every wireless section interface, and you may have them one [at a time] for every (every subunit classification) subunit (also including a substitute).

[0117] Although it assumes that Acert and Bcert are the authentication formats which

the same certificate authority (for example, certificate authority which takes charge of the copy protection of IEEE1394) published here, you may be the authentication format which another certificate authority which this certificate authority may similarly publish about an authentication format (Ccert and Dcert which are mentioned later) of the wireless section mentioned later, and takes charge of the wireless section publishes.

[0118] Next, an example of the internal structure of the wireless node 2103 is shown in drawing 23 . It is the same as that of the wireless node of the 1st operation gestalt fundamentally except the copy protection processing section 2303 having the authentication format Dcert for the wireless sections.

[0119] Next, the sequence of the whole MPEG image after performing actual copy protection is explained, referring to drawing 24 / drawing 25 (the whole example of a sequence), drawing 26 / drawing 27 (example of a flow chart of the transmitting node 2101), drawing 28 / drawing 29 / drawing 30 / drawing 31 (example of a flow chart of the junction node 2102), and drawing 32 / drawing 33 (example of a flow chart of the wireless node 2103).

[0120] First, the wireless node 2103 notifies its configuration information to the junction node 2102 (step S2501). having [a one (wireless node)]-with configuration information-MPEG decoding / display function ****** -- it is things, having the authentication format for authentication, etc. (refer to drawing 14). Here, the authentication format for authentication may notify the purport which is the authentication format for the wireless sections (step S2801).

[0121] The junction node 2102 which received this checks that the wireless node 2101 has an authentication format or having MPEG decoding / display function (step S2701). The junction node 2102 advertises this MPEG decoding / display function to an IEEE1394 bus side as a subunit of junction node 2102 self like the 1st operation gestalt using IEEE1212 register, an AV/C protocol, etc. (step S2502).

[0122] Therefore, the junction node 2102 has the substitute table 2214 in the substitute subunit configuration section 2210. This substitute table 2214 is the same as that of the 1st operation gestalt fundamentally, and is a table which matching with the form which the junction node 2102 is advertising in the substitute, and its stereo is describing like drawing 34 / drawing 35 .

[0123] Here, the substitute advertisement of the MPEG decoding / display function of the wireless node 2103 is carried out as an own subunit of a junction node like drawing 34 (steps S2702 and S2703).

[0124] For this reason, the structure of the junction node 2102 seen from the transmitting node 2101 will look like drawing 36 (step S2601).

[0125] Although the above was explanation about an IEEE1394 bus side, the same relation as this is realized like the 1st operation gestalt also at the wireless section. That is, the junction node 2102 investigates the device by the side of an IEEE1394 bus, service, a subunit configuration, etc., and is offering these substitute services to the wireless section side. Therefore, a setup like drawing 35 is made and the structure of the junction node 2102 seen from the wireless node looks like drawing 37 .

[0126] Now, the transmitting node 2101 recognized that MPEG decoding / display subunit is in the junction node 2102 a purpose [transmit / to this subunit / an MPEG image] -- a 1394 bus top -- synchronous channel #x -- being established -- an AV/C protocol -- "-- with this synchronous channel #x (plug to receive) MPEG decoding / display subunit is connected and the instruction with display an image" is issued (steps S2503 and S2602). Since the transmitting node 2101 is interpreting it as what has this subunit in the junction node 2102, the transmission place of an instruction is the junction node 2102.

[0127] The junction node 2102 which received this (step S2704) interprets the instruction packet which received, recognizes that that instruction is an instruction to MPEG decoding / display subunit to which oneself is offering substitute service, and recognizes that the stereo of this instruction place is in the wireless node 2103 with reference to the substitute table 2210 (step S2705).

[0128] Here, the wireless section of drawing 20 is the wireless LAN corresponding to QOS, and if the procedure defined beforehand is completed, it will presuppose that there is no quality degradation of packet abandonment, delay, etc., and it is possible to transmit transfer data to a transmission place. On this wireless LAN, data are transmitted like drawing 38 with a wireless frame with the same format as an Ethernet frame, i.e., a format like "the transmitting agency address, a destination address, and data."

[0129] Now, a QOS setup of the wireless section is performed that it should act to a wireless node side as the forward of the data received through synchronous channel #x of an IEEE1394 bus. Furthermore, the ISO signal sender and receiver 2203 (synchronous channel #x are received) and the wireless ISO signal sender and receiver 2206 (it transmits with the wireless frame which offers a QOS guarantee) are connected like the dotted line of drawing 22 (since a decryption of a code cannot be performed yet), and it is made to carry out at the wireless section the forward of the ISO input data inputted from 1394 interfaces 2201 as it is (steps S2504, S2706, and S2707).

[0130] Furthermore, the instruction with "since it lets the above-mentioned wireless frame pass and data are transmitted, receive this and display the result on a display" is

transmitted in the form of a wireless node control packet to the wireless node 2103 (steps S2505, S2708, and S2802). An IEEE1394AV/C protocol or IEC61883 protocol, and the thing that transformed these may be used for this control protocol. the data transmitted with this operation gestalt although there is no concept of a synchronous channel on wireless LAN so that it may mention later -- the source -- ID (SID) -- a field is prepared, the QOS data which have transmitted QOS data to the wireless section and which have been transmitted for every node can be uniquely distinguished now, and this value of SID can be used for distinction of data flow like the synchronous channel of IEEE1394. An example of a wireless node control packet is shown in drawing 39 . The transmitting origin of a packet is the junction node 2102.

[0131] the wireless node 2103 which received this -- alpha -- it recognizes that SID is given and the QOS transfer of the data is carried out.

[0132] Then, the transmitting node 2101 lets synchronous channel #x pass, and transmits the enciphered MPEG image (steps S2506 and S2603). A contents key is set to K1. This cryptographic key is drawn as the exchange key mentioned later or seed's function.

[0133] Moreover, the "transmitting node ID" which identifies a transmitting node besides a synchronous channel number may be contained in the frame which transmits this enciphered MPEG image.

[0134] While the junction node 2102 which received this recognizes that data are enciphered For example, with reference to the "transmitting node ID" contained in received data, recognize that the transmitting node 2101 has transmitted this data (step S2709), and the transmitting node 2101 is received. In order to confirm "You let synchronous channel #x pass. Whether the subunit of transmitting node 2101 throat has sent out this data", the inquiry of an authentication place is performed (steps S2507 and S2710). Under the present circumstances, the synchronous channel number (#x) to which data are transmitted is indicated, and while the transmitting node 2101 enables it to specify the subunit which has transmitted data, the subunit (in the case of this operation gestalt subunit ID= of MPEG decoding / display subunit of the junction node 2102 0) of the self which receives this data is also notified. This has the role which notifies the authentication place seen from the transmitting node 2101.

[0135] In addition, this authentication place inquiry packet and the authentication place response packet mentioned later indicate the data hashed and enciphered as electronic signature with the private key of a certificate authority, and may enable it to check that there is no alteration etc.

[0136] Now, the transmitting node 2101 which received the authentication place inquiry

(step S2604) While the subunit which has received the data transmitted to synchronous channel #x recognizes that it is MPEG decoding / display subunit of the junction node 2102 oneself -- this -- the subunit which has transmitted to synchronous channel #x notifies that it is an image transmitting subunit (subunit ID=0) to the junction node 2102 as an authentication place response packet (steps S2508 and S2605).

[0137] Thereby, the junction node 2102 can recognize that the subunit which has transmitted data to synchronous channel #x is an image transmitting subunit (subunit ID=0) of the transmitting node 2101 (step S2711).

[0138] The junction node 2102 (redundancy of MPEG decoding / display subunit) the subunit which has transmitted data to synchronous channel #x has recognized it to be that it is the image transmitting subunit of the transmitting node 2101 performs an authentication demand to the image transmitting subunit of the transmitting node 2101 continuously. An authentication format (Bcert) of MPEG decoding / display subunit of a junction node or a junction node is transmitted to this authentication demand both (steps S2509, S2606, S2607, and S2712). Like the 1st operation gestalt, exchange of this authentication demand and an authentication format is performed, even if it turns to the junction node 2102 (MPEG decoding / display subunit) from the transmitting node 2101 (image transmitting subunit) (steps S2510, S2608, S2713, and S2714). Thus, if the subunits with which the communication link of the same equipments is also communicating differ, also in the 2nd operation gestalt, the information about a subunit will also be exchanged for authentication and key exchange, because it can be made to perform use of a different key.

[0139] Both the nodes that authentication completed to each other perform authentication and key exchange procedure like the 1st operation gestalt (steps S25111, S25112, S2609, and S2715), and share the authentication key Kauth1. Using this authentication key, the transmitting node 2101 can perform a transfer of an exchange key and seed to the junction node 2102 (steps S2512, S2610, and S2716), and can know now the value of the contents key K1 by the junction node 2102 after all (step S2717).

[0140] Henceforth, the MPEG image (synchronous channel #x course) (steps S2513, S2611, and S2612) enciphered with the contents key K1 transmitted It is decrypted by the junction node 2102 (steps S2514 and S2718). Furthermore, it is re-enciphered with the contents key k2 independently prepared in the wireless sections (steps S2515, S2516, and S2719), and is transmitted to the wireless node 2103 in the form where a wireless section top is guaranteed to QOS (steps S2517, S2720, and S2803). An MPEG image passes along pass called the ISO signal sender and receiver 2203, the code decryption section 2204, the encryption section 2205, and the wireless ISO signal sender

and receiver 2206 at this time.

[0141] as stated previously, in order to be able to perform distinction of the data which the junction node 2102 has transmitted to the wireless section side at this time -- the source -- ID -- a meaning value may be given and sent out by the junction node 2102. Here, this meaning value is set to alpha. That is, the data which the value of alpha attached are data (what decrypted with the contents key K1 and was re-enciphered with the contents key K2) received from synchronous channel #x of IEEE1394. The junction node 2102 recognizes that the data which attached SID of alpha and have been sent out at the wireless section are data transmitted from the redundancy of the image transmitting subunit by the side of the own wireless section.

[0142] Actuation of the wireless node 2103 which received this is the same as actuation of the junction node 2102 which received the encryption data explained previously fundamentally. Namely, while recognizing that data are enciphered, the "transmitting agency address" included, for example in received data is referred to. the junction node 2102 has transmitted this data -- recognizing -- the junction node 2102 -- receiving -- "alpha -- having given the value and having sent out this data In order to confirm whether it is the subunit of junction node 2102 throat", the inquiry of an authentication place is performed to a junction node (steps S2518 and S2804).

[0143] Under the present circumstances, the value (alpha) of SID to which data are transmitted is indicated, and while the junction node 2102 enables it to specify the subunit which has transmitted data, the subunit (in the case of this operation gestalt subunit ID= of MPEG decoding / display subunit of the wireless node 2103 0) of the receiving side which receives this data is also notified. This has the role which notifies the authentication place seen from the junction node 2102.

[0144] The junction node 2102 which received the authentication place inquiry (step S2721) While the subunit which has received the data transmitted to SID=alpha recognizes that it is MPEG decoding / display subunit (subunit ID=0) of the wireless node 2103 The subunit which oneself gave SID=alpha and has transmitted notifies that it is an image transmitting subunit to the wireless node 2103 as an authentication place response packet (steps S2519, S2722, and S2805).

[0145] Thereby, the subunit which the wireless node 2103 gave SID=alpha and has transmitted data can recognize that it is the image transmitting subunit of the junction node 2102.

[0146] The wireless node 2103 (MPEG decoding / display subunit) the subunit which gave SID=alpha and has transmitted data has recognized it to be that it is the image transmitting subunit of the junction node 2102 performs an authentication demand to

the image transmitting subunit of the junction node 2102 continuously (steps S2520, S2723, S2724, and S2806). An authentication format (Dcert) of a wireless node (or MPEG decoding / display subunit of a wireless node) is transmitted to this authentication demand both. Exchange of this authentication demand and an authentication format is performed even if it turns to the wireless node 2103 (MPEG decoding / display subunit) from the junction node 2102 (image transmitting subunit) (steps S2521, S2725, and S2807).

[0147] Both the nodes that authentication completed to each other perform authentication and key exchange procedure continuously (steps S2522, S2523, S2726, and S2808), and share the authentication key Kauth2. Using this authentication key, the junction node 2102 performs a transfer of an exchange key and seed to the wireless node 2103 (steps S2524, S2727, and S2809), after all, is the wireless node 2103 and can know now the value of the contents key K2 (step S2810).

[0148] In addition, it is also possible for reverse sequence to be sufficient and to perform both in parallel at old explanation, although the form performed one by one explained the authentication and key exchange between a transmitting node and a junction node, and the authentication and key exchange between a junction node and a wireless node.

[0149] Henceforth, the MPEG image (step S2525) enciphered with the contents key K1 transmitted In the form where it is decrypted by the junction node 2102 (step S2526), and is re-enciphered with the contents key K2 further prepared for the wireless sections independently (steps S2527, S2528, and S2728), and a wireless section top is guaranteed to QOS It is transmitted to the wireless node 2103 in the form of a wireless frame where SID=alpha was given (steps S2529 and S2729).

[0150] Shortly, since the wireless node 2103 can calculate the contents key K2 using the exchange key which came to hand previously, and seed's value, it is possible to decrypt this (steps S2530 and S2811), and this is reproduced in the display section 2307 (step S2812).

[0151] Also in an IEEE1394 bus, that of a wireless network, and the environment of interconnect where a substitute node exists in between, the junction node which offers redundancy, a transmitting node, and a junction node and a receiving node thus, in each section By performing authentication procedure and key exchange procedure, it is enciphered in all the paths that it cannot copy, the required data transfer of contents protection, such as an actual MPEG image, can be performed, and safe data transfer is possible. The data transfer which took copy protection into consideration also in the environment of such interconnect by this becomes possible.

[0152] On the part and concrete target with which "the raw MPEG data" of the junction

node 2102 flows, of course, between the code decryption section 2204 and the encryption section 2205 Since risk of data being copied can be considered, if the device (for example, the code decryption section and the encryption section are set to LSI of one) not to make a data copy in this part is made Since it becomes impossible substantially for a probe to be applied between them and to intercept data (illegal copy), it is useful to perform such a cure.

[0153] (3rd operation gestalt) Next, the 3rd operation gestalt is explained.

[0154] It is an operation gestalt when the AV equipment control software equivalent to the high order layer of AV/C represented with the 3rd operation gestalt by HAVI specification (Specification of the Home Audio/Vidio Interoperability(HAVI) Architecture) etc. on IEEE1394 is working.

[0155] An example of the whole configuration of the home network of a certain home is shown in drawing 40 . This whole configuration is the same as that of the 1st operation gestalt fundamentally.

[0156] An example of the internal structure of the transmitting node 4101 is shown in drawing 41 . Although this is the same as that of the case of the 1st operation gestalt almost, additional description is carried out for emphasis of IEEE1212 register 4407. Information, such as the attribute of the transmitting node 4101, for example, "Arrangement URL and the control icon of the information which shows the product of what kind of genres, such as the information which shows of which vendor it is a product, for example, VTR, and a tuner, a serial number, and the control software, a command list", etc., is included in IEEE1212 register 4407.

[0157] Next, an example of the internal structure of the junction node 4102 is shown in drawing 42 . Although the junction node 4102 is also the almost same configuration as the 1st operation gestalt, the point of having described IEEE1212 required register 4213 especially into the 1394 bus-arrangement recognition section 4206 when explaining the sequence of this operation gestalt, and a point with the HAVI processing section 4212 differ from the 1st operation gestalt. The virtual machine (VM) which processes the so-called HAVI cutting tool code exists in the HAVI processing section 4212. Moreover, in this operation gestalt, the substitute subunit configuration section 4207 has the redundancy of the "panel subunit" which describes a control screen.

[0158] Next, an example of the internal structure of the wireless node 4103 is shown in drawing 43 . The same is fundamentally [as the case of the 1st operation gestalt] said of this.

[0159] Next, the sequence of the whole MPEG image after performing actual copy protection in the HAVI environment is explained, referring to drawing 44 / drawing 45

(the whole example of a sequence), drawing 46 / drawing 47 (example of a flow chart of the transmitting node 4101), drawing 48 / drawing 49 / drawing 50 (example of a flow chart of the junction node 4102), and drawing 51 / drawing 52 (example of a flow chart of the wireless node 4103).

[0160] First, the wireless node 4103 notifies its configuration information to the junction node 4102 (step S4501). At this time, such configuration information shall be sent to the junction node 4101 as information on an IEEE1212 register format. That is, the junction node 4102 requires "the information about the part equivalent to this address of the CSR (command status register) space specified in IEEE1212" from the wireless node 4103, and this exchange may be performed in the form where the wireless node 4103 replies to this. Here, that a them (wireless node) has MPEG decoding / display function, having the authentication format for authentication, etc. are included in this configuration information as mentioned above. Here, the authentication format which the wireless node 4103 has is set to Bcert.

[0161] The junction node 4102 which received this checks that the wireless node 4101 has an authentication format or having MPEG decoding / display function (step S4701). The junction node 4102 advertises this MPEG decoding / display function to an IEEE1394 bus side as a subunit of junction node 4102 self, in order that the wireless node 4101 may tell having MPEG decoding / display function to the node by the side of an IEEE1394 bus (step S4502). The purport "he has MPEG decoding / display function" in IEEE1212 own register is indicated, or when an AV/C protocol receives an inquiry of a subunit function, specifically, a response is returned in the form where he has MPEG decoding / display subunit (the node connected to IEEE1394 of transmitting node 4101 grade will recognize it as this function existing in a junction node by this).

[0162] Therefore, the junction node 4102 has the substitute table 4208. The substitute table 4208 is a table which matching with the form which the junction node 4102 is advertising in the substitute, and its stereo is describing like drawing 53 / drawing 54 .

[0163] Here, the substitute advertisement of the MPEG decoding / display function of the wireless node 4103 is carried out as an own subunit of a junction node like drawing 53 (steps S4702 and S4703).

[0164] Procedure contrary to the above is performed in the form where substitute registration of the transmitting node 4101 on the IEEE1394 bus 4104 is shown to a wireless section side (steps S4503 and S4504). That is, it describes that he has an image transmitting function and having a panel feature (control screen function) to IEEE1212 register 4407 of the transmitting node 4101, and the junction node 4102 reads this into it (steps S4601 and S4704). As a function of the junction node 4102, it acts for the

function of this transmitting node 4101, and I reflect it in the 1212 about IEEE function by the side of the wireless section (CSR space by the side of the wireless section), and have you recognize to the wireless node 4103 side as that the above-mentioned image transmitting function and whose panel feature are functions of the junction node 4102. This correspondence relation is reflected in the substitute table 4208 like drawing 54 (step S4705).

[0165] Thus, the substitute table 4208 is constituted like drawing 53 / drawing 54 . Moreover, the internal structure of the junction node 4102 which looked at the internal structure of the junction node 4102 seen from the transmitting node 4101 from the wireless node 4103 to drawing 55 is shown in drawing 56 , respectively.

[0166] In addition, the cutting tool code of HAVI for controlling the transmitting node 4101 is contained in the transmitting node configuration information of step S4503 at this time, and the junction node 4102 may have the substitute server of the transmitting node 4101, i.e., the function of DCM (device control module). In this case, this cutting tool code will work on the virtual machine in the HAVI processing section 4212 of the junction node 4102.

[0167] Now, the wireless node 4103 recognized to be a thing with a panel feature sends out the command of a display demand of a panel to the junction node 4102 to the (panel subunit) of the junction node 4102 (steps S4505 and S4802). The junction node 4102 which received this (step S4706) recognizes that the stereo of this panel feature exists in the transmitting node 4101 with reference to the substitute table 4208, and acts as the forward of said panel display demand command to the transmitting node 4101 (steps S4506 and S4707).

[0168] The transmitting node 4101 which received this (step S4601) performs a panel response (that is, transmission of a control screen) with an AV/C protocol. A transmission place is the junction node 4102 (steps S4603 and S4507). The junction node 4102 which received this (step S4708) acts to the wireless node 4103 as the forward of this with reference to the substitute table 4208 (steps S4709, S4508, and S4803).

[0169] Here, an example of the control screen sent to drawing 57 at the wireless node 4103 is shown. On this control screen (panel), the carbon button which displayed the title of six movies is offered. These carbon buttons shall serve as structure sent to the transmitting origin of a panel, for example in the form of the command "the carbon button 1 was pushed", if the carbon button which identifiers, such as "a carbon button 1", "a carbon button 2", and --, are attached, and has a user is pushed.

[0170] Now, it thinks that the image transmitting service recognized that the junction

node 4102 offers the wireless node 4103 will be received (what is actually offered is the transmitting node 4101), wireless synchronous channel #y for passing an image is secured using a wireless node control packet (step S4509), and the command for connecting this channel to the image transmitting subunit of the junction node 4102 is published to the junction node 4102 (step S4804). The junction node 4102 which received this refers to the substitute table 4208. While checking the node (transmitting node 4191) by which this AV/C command should actually be published and securing a band required on an IEEE1394 bus (synchronous channel #x), the internal ISO signal sender and receiver 4204 is set up. Synchronous channel #x and wireless synchronous channel #y of an IEEE1394 bus are connected mutually (steps S4710, S4711, S4712, and S4510). Moreover, the junction node 4102 publishes the command which connects synchronous channel #x to an image transmitting subunit to the transmitting node 4101 (steps S4511 and S4713). The transmitting node 4101 which received this (step S4604) connects to synchronous channel #x of an IEEE1394 bus the pass (part which is a double arrow head by drawing 41) with which the image stream of the interior which is the stereo of an image transmitting subunit flows.

[0171] It gets mixed up with this, and the user of the wireless node 4103 pushes the carbon button of a control screen that a suitable program should be chosen out of the panel of drawing 57 , in order to choose an image to see (for example, it touches [clicking using a mouse, carrying out a pen input,]). This actuation is transmitted to the junction node 4102, and this is changed into the command to the transmitting node 4101 through reference of the substitute table 4208 (steps S4805, S4714, S4715, S4605, S4512, and S4513).

[0172] Then, the transmitting node 4101 lets synchronous channel #x pass, and transmits the enciphered MPEG image (steps S4514 and S4606). This is relayed by the junction node 4102 and reaches the wireless node 4103 (step S4716).

[0173] the MPEG image which that of a next procedure is the same as that of the case of the 1st operation gestalt, and was enciphered -- the wireless node 4103 -- reaching (step S4806) -- at this time, since the wireless node 4103 does not have the key for solving this code, it starts authentication procedure the transmitting origin of an MPEG image. Since it is the same as that of the 1st operation gestalt about the procedure after authentication procedure, detailed explanation here is omitted.

[0174] in addition, the function in which authentication is equivalent to the image transmitting subunit of the transmitting node 4101 if the 1st operation gestalt is followed and the function equivalent to the image receiving subunit of a wireless node -- ** -- although it is thought that it is carried out in between, in the case of the 3rd

operation gestalt, a method with which the panel subunit of the transmitting node 4101 is set as the object of authentication at everything but such an authentication method is also considered. In this case, a device ID will be assigned to the panel of the transmitting node 4101.

[0175] In addition, in HAVI, the control screen information for controlling the transmitting node 4101 may be contained in DCM which is the cutting tool code sent from the transmitting node 4101. Such a module is called DDI (data driven interaction). Such a module is developed in the HAVI processing section 4212 in the junction node 4102, and a control screen is generated. Although it is necessary to consider showing this control screen (or control screen with a function equivalent to it) as a wireless node side with this operation gestalt In this case, the substitute subunit configuration section 4207 recognizes the screen configuration information contained in this DDI (for example, carry out the event of the system call for a screen configuration, and it is recognized). This control screen is reconfigurated as a panel which can consider how to guess the outline of the last screen generated, the approach based on the completed control screen, etc., and how to open this to the wireless section as a "panel subunit" can be considered. In this case, this panel and the correspondence table of HAVI or the command (published from the junction node 4102 to the transmitting node 4101) of AV/C which should be generated by DDI will be prepared for the substitute table 4208. Even if the virtual machine of a HAVI cutting tool code does not exist in the wireless node 4103, since it is effective, this approach is the approach of enabling control of a HAVI device from the wireless node 4103 without a HAVI virtual machine.

[0176] (4th operation gestalt) Next, the 4th operation gestalt is explained.

[0177] An example of the whole configuration of this operation gestalt is shown in drawing 58 .

[0178] As shown in drawing 58 , with the 4th operation gestalt, the IEEE1394 bus 6104 which is the home network of a certain home, and a public network (here, a telephone network etc. may be used although considered as the Internet as an example) 6105 are connected in the home gateway 6102, and after passing through authentication procedure and the procedure of encryption between the transmitting node 6101 and the receiving node 6103, image data are exchanged. Here, the Internet 6105 (a part for an access mesh part) has a very thin communication band compared with the IEEE1394 bus 6104, and the image information (suppose that it is an MPEG 2 image as an example) exchanged by IEEE1394 bus considers transmitting, after performing code translation from transformer coding, i.e., an MPEG 2 sign, to an MPEG4 sign in the home gateway 6102, since it cannot let a band pass, without being insufficient.

[0179] Also in the 4th operation gestalt, termination of the exchange, a series of copy protection procedure, i.e., authentication procedure, of encryption data is carried out like the 2nd operation gestalt in the home gateway. That is, copy protection procedure is respectively closed by the transmitting node, and the home gateway and a home gate wait receiving node. Also in this operation gestalt, the home gateway offers substitute service to a transmitting node or a receiving node, and the home gateway itself has an authentication format about copy protection, and the home gateway itself carries out termination of each responsibility about an MPEG data encryption transfer of the 1394 bus sections and the wireless section.

[0180] Next, an example of the internal structure of the transmitting node 6101 is shown in drawing 59 . This is the same configuration as an old operation gestalt fundamentally.

[0181] Next, an example of the internal structure of the home gateway 6102 is shown in drawing 60 .

[0182] The fundamental configuration of the home gateway 6102 is the same as the configuration of the junction node of the 2nd operation gestalt almost, if the point of having the point and not the substitute subunit configuration section but substitute homepage creation section 6210 which has not a wireless interface but the Internet interface 6202, the point of having creation / are recording section 6211 of a homepage, and the point of having MPEG 2 / MPEG4 transducer 6214 between the code decryption section 6204 and the encryption section 6205 are removed. Sequential explanation is given about the above-mentioned difference.

[0183] The home gateway 6102 serves as a substitute server of the node by the side of an IEEE1394 bus (this operation gestalt transmitting node 2101) to the node by the side of the Internet, and has the function to offer the function of the node by the side of an IEEE1394 bus in a substitute. It is possible to access service (image transmitting service when it is this operation gestalt) which the transmitting node 6101 offers through the homepage which the home gateway 6102 offers. Here, from the receiving node 6103, since it is visible through the homepage of the home gateway 6102, service of the transmitting node 6101 may be interpreted as service on IP (Internet) which the home gateway 6102 provides with this.

[0184] Moreover, although the home gateway 6102 has the function which acts to the Internet side as the forward of the data (MPEG 2 image data) received from the IEEE1394 bus side like the 2nd operation gestalt, in this home gateway 6102, termination of the procedure about copy protection, such as authentication and a data encryption, is carried out about both the IEEE1394 bus section and the Internet section.

About an IEEE1394 bus side, the authentication format Bcert in the IEEE1394 copy protection processing section 6208 about the Internet section side It has the authentication format Ccert in the Internet side copy protection processing section 6212, respectively. About the encryption data inputted from the synchronous channel of an IEEE1394 bus To the ISO signal sender and receiver 6203 ****** -> A transformer code ->MPEG4 image is transmitted for the MPEG 2 image decrypted [which were decrypted and was code-decrypted] in the code decryption section 2204 to the Internet side in the encryption section 6205 by MPEG 2 / MPEG4 transducer 6214 in the re-encryption ->AV signal sender and receiver 6206. The process to say is stepped on.

[0185] Although it assumes that Acert and Bcert are the authentication formats which the same certificate authority (for example, certificate authority which takes charge of the copy protection of IEEE1394) published here, you may be the authentication format which another certificate authority which this certificate authority may similarly publish about an authentication format (Ccert and Dcert which are mentioned later) of the Internet section mentioned later, and takes charge of the Internet section publishes.

[0186] In addition, in this operation gestalt, it may not have an authentication format (Acert-Dcert) in every [one] node (or network interface), but you may have it one for every subunit (every subunit classification) and every Internet application. That is, a different authentication format may be used in different Internet application. Here, a flow points out a series of data styles expressed in the group of the (the transmitting address, the transmit port, the receiving address, and the receive port) of the Internet.

[0187] Next, an example of the internal structure of the receiving node 6103 is shown in drawing 61 .

[0188] The copy protection processing section 6303 has the authentication format Dcert for the Internet. The difference with the 2nd operation gestalt is a point that the interface (the Internet interface 6301, the control packet transceiver section 6302, AV signal sender and receiver 6304) serves as Internet-compatible. Here, the control packet transceiver section 6302 may be a transceiver module of a packet in which TCP and the AV signal sender and receiver 6394 have the transport protocol of UDP.

[0189] Next, the sequence of the whole image transmission after performing actual copy protection is explained, referring to drawing 62 / drawing 63 (the whole example of a sequence), drawing 64 / drawing 65 (example of a flow chart of the transmitting node 6103), drawing 66 / drawing 67 / drawing 68 / drawing 69 (example of a flow chart of the home gateway 6102), and drawing 70 / drawing 71 (example of a flow chart of the receiving node 6103).

[0190] First, the home gateway 6102 lets reading of IEEE1212 register of the

transmitting node 6101 etc. pass, and collects the attribute about a transmitting node, and configuration information (steps S6501, S6601, S6701, S6502, S6602, and S6702). Letting this pass, the home gateway 6102 grasps that the transmitting node 6101 has an image transmitting function, having a panel feature, having an authentication format, etc.

[0191] In response, the home gateway 6102 creates the homepage for carrying out remote control of the transmitting node 6101 (step S6503). Fundamentally, the same screen as the panel which the transmitting node 6101 has is created as "a homepage for transmitting node control." It carries out that the carbon button for control arranged on a homepage is equivalent to the carbon button of the panel subunit of the transmitting node 6101, respectively etc., and the list of correspondence is described by the translation table in the substitute homepage creation section 6210. For example, when "playback" and the carbon button which has withered exist in the panel subunit of the transmitting node 6101, "playback" and the carbon button which has withered are prepared also for this homepage, and this relation is described to said translation table. When the user of this homepage pushes this carbon button, it becomes the form where the interaction "the carbon button was pushed" returns to "playback" carbon button of the panel subunit of the transmitting node 6101 from the home gateway 6102. An example of the homepage for transmitting node control to which the home gateway 6102 created an example of the panel which the panel subunit of the transmitting node 6101 has in drawing 72 (a) to drawing 72 (b) is shown, respectively.

[0192] Now, the receiving node 6103 on the Internet accesses this home gateway 6201 through the Internet, a homepage including the control screen of the transmitting node 6101 is required, and this homepage is sent (steps S6504, S6801, and S6703). Seeing this, the user of the receiving node 6103 should push the carbon button (for example, "playback" carbon button of drawing 72 (b)) which requires the image transmission on a screen. As a result, for example, the interaction "the playback carbon button was pushed", it is notified to the home gateway through HTTP via the Internet (steps S6505, S6802, and S6704).

[0193] IP flow to which the stream which gets mixed up with this notice and is exchanged between a home gateway 6102 and the receiving node 6103 is transmitted -- that is, (a transmitting IP address, a transmit port, a receiving IP address, receive port), the decision of a group, the negotiation of session control (a coding method, authentication method, etc.), etc. are performed (steps S6505, S6705, and S6803). For example, the decision of a coding method, the method of authentication, and the number of a port etc. is made using RTSP (real-time transport streaming protocol), SDP (session

desk RIPUSHON protocol), etc.

[0194] In response to these processings, a home gateway 6102 recognizes that the stereo which performs image transmission is the image transmitting subunit of the transmitting node 6101, to the transmitting node 6101, is an AV/C protocol etc. and publishes commands, such as a demand of image transmission, to a setup of synchronous channel #x for data transfer, and an image transmitting subunit (step S6506).

[0195] In response, from the transmitting node 6101, it lets synchronous channel #x pass and the enciphered MPEG image is sent out to a home gateway 6102 (steps S6507, S6603, and S6604). It is a procedure by the side of IEEE1394 of the 2nd operation gestalt, and the same procedure, an authentication place inquiry / response, an authentication demand, authentication and key exchange procedure, an exchange key / seed transfer, etc. are performed, and it comes to be able to perform count of the contents key K1 in a home gateway 6102 after that (step S6508- S6514, S6605-S6611, S6706-S6715).

[0196] Henceforth, the home gateway 6102 which received the MPEG image (steps S6515, S6612, and S6613) enciphered through synchronous channel #x decrypts this on an MPEG 2 image in the code decryption section 6204 using the contents key K1 (steps S6516, S6517, and S6716). Next, the transformer code of the extracted MPEG 2 image is carried out to an MPEG4 image by MPEG 2 / MPEG4 transducer 6214 (step S6518). This MPEG4 image is re-enciphered in the encryption section 6205 using the contents key K2 (steps S6519, S6520, S6717, and S6718), and this is IP-packet-ized. In that case, as decided in the procedure of previous session control, as for C (IP address of a home gateway), and a transmit-port number, c and a receiving IP address generate [a transmitting IP address] an IP packet [as / D (IP address of a receiving node) and whose receive-port number are d] (steps S6521 and S6719).

[0197] The receiving node 6103 which received this recognizes that the received data are enciphered (step S6804). The receiving node 6103 recognizes that the home gateway 6102 has transmitted this data by referring to IP header of the packet which arrived etc., and an authentication demand is transmitted to a home gateway 6102 (steps S6522 and S6805). An IP packet is sufficient also as the packet of this authentication demand. The number currently beforehand assigned to the procedure which attests may be used for the port number for an authentication demand. Under the present circumstances, the flow ID of a stream transmission (C, c, D, d) is given and transmitted to the packet of this authentication demand. By this, a home gateway 6102 can recognize the authentication demand to which flow it is. Although illustration has not been carried

out, the authentication format (for these streams) of a receiving node etc. is included in this authentication demand.

[0198] Moreover, you may tell using RTP (Realtime Transport Protocol) as a transport protocol etc. to coincidence.

[0199] In response, it recognizes that a home gateway 6102 is the authentication demand for a flow (C, c, D, d), and the authentication demand including the authentication format for this flow is returned to a receiving node (steps S6523, S6720-S6722, S6806, S6807). At this time, said flow ID etc. is included in this authentication demand.

[0200] Next, both perform a transfer of authentication and key exchange procedure, and an exchange key / seed etc. on an IP packet (step S6524- S6526, S6723, S6724, S6808-S6810). Thereby, the receiving node 6103 can generate the contents key K2 now.

[0201] Therefore, the MPEG4 data (step S6527- S6533, S6725, S6726, S6811) which were enciphered with the contents key K2 and which are sent through a flow (C, c, D, d) become possible [decrypting with the contents key k2 prepared as mentioned above] henceforth (step S6534). The decrypted MPEG4 data are decrypted in the MPEG decoding section 6306 (step S6812), and reproduce this in the display section 6307 (step S6813).

[0202] Thus, also in the environment where a home network and the Internet interconnected, it is enciphered in all the paths that it cannot copy, the required data transfer of contents protection, such as an actual MPEG image, can be performed, and safe data transfer is possible because the home gateway and the transmitting node which offer redundancy, and the home gateway and a receiving node perform authentication procedure and key exchange procedure. Thus, also in the environment of such interconnect, it becomes possible to perform data transfer in consideration of copy protection.

[0203] In the home gateway 6102, the cure of closing to a device, for example, LSI of one, specifically not making [the part into which "raw MPEG data" flows, and] a data copy between the code decryption section 6204, the MPEG 2 / MPEG4 transducer 6214, and the encryption section 6205 may be formed like the 2nd operation gestalt.

[0204] (5th operation gestalt) Next, the 5th operation gestalt is explained.

[0205] It is the case where the 5th operation gestalt exchanges contents between home networks through a public network to the 4th operation gestalt having been the case where contents were exchanged, between the terminal of the home screen oversize after accessing the home network through the public network (Internet) and taking copy protection into consideration, and the terminal on the Internet.

[0206] This whole operation gestalt block diagram is shown in drawing 73 .

[0207] As shown in drawing 73 , with the 5th operation gestalt, two home networks 8105 and 8107 are connected with the public network (here, B-ISDN etc. is sufficient although considered as the Internet as an example) 8106. From the transmitting node 8101 on the 1st home network 8105, AV contents are transmitted to the receiving node 8104 on the 2nd home network 8107 in the form where copy protection was taken into consideration. Here, although the 4th operation gestalt showed the example when the communication band of a public network part is very thin, with this operation gestalt, the communication band of a public network shall have sufficient capacity.

[0208] In the 5th operation gestalt, substitute service of the service on the IEEE1394 bus 8105 and 8107 is carried out like the junction node of the 1st operation gestalt in the home gateways 8102 and 8103 at a public network side. That is, from on the Internet, the equipment of a home screen oversize, and service and contents can be seen as service of the Internet. Moreover, the home gateways 8102 and 8103 act as the forward of these about an exchange, a series of copy protection procedure, i.e., authentication procedure, of encryption data.

[0209] The transmitting node 8101 and the receiving node 8104 are the same configurations as the 4th operation gestalt fundamentally.

[0210] An example of the internal structure of the home gateways 8102 and 8103 is shown in drawing 74 .

[0211] The fundamental configuration of the home gateway 8102 is the same as the configuration of the home gateway of the 4th operation gestalt almost except for the point (this is the same as that of the junction node of the 1st operation gestalt) which does not carry out termination of the copy protection, and the point (this is the same as that of the junction node of the 1st operation gestalt) of not performing coding, decryption, and code translation of a code.

[0212] An example of the whole sequence is shown in drawing 75 .

[0213] Here, the case where the user of the 2nd home network 8107 makes the contents of the transmitting node 8101 distribute to the receiving node 8104 through the Internet 8106 using the control screen of the home gateway 8103 is considered.

[0214] First, configuration recognition of step S8301 and homepage creation for transmitting node control of step S8302 are performed like the 4th operation gestalt.

[0215] The user of the 2nd home network 8107 operates the home gateway 8103, and brings the homepage for transmitting node control (control screen) from the home gateway 8102 (step S8303). Moreover, the control screen of the receiving node 8104 which is illustrated, for example to drawing 76 is also opened to coincidence. Then, like

drawing 76 , a suitable thing is dragged and dropped from the contents list in a transmitting node, for example, and video delivery through the Internet is ordered to the home gateway 8103 (step S8304).

[0216] Then, an image Request to Send is published like the 4th operation gestalt in the home gateway 8102 (step S8305). (as the Internet command) This is translated into an AV/C protocol command in the home gateway 8102. The communication path between the receiving nodes 8104 (synchronous channel #y on synchronous channel #x on the IEEE1394 bus 8105, the connection on the Internet, and an IEEE1394 bus) is set up from the transmitting node 8101 (steps S8306 and S8307). Besides, the MPEG 2 image enciphered by the cryptographic key K is distributed (steps S8308-S8310).

[0217] The receiving node 8106 which received this publishes an authentication demand to a transmitting agency like the 1st operation gestalt (step S8311). Since the receiving node 8104 is interpreting it as this image being distributed from the home gateway 8103, this authentication demand is given to the home gateway 8103.

[0218] The home gateway 8103 acts to the home gateway 8102 as the forward of this with reference to the internal translation table 8211 like the 4th operation gestalt. It is because this is interpreting the home gateway 8103 as the distribution origin of an image being the home gateway 8102. This forward is performed by the Internet packet in the form where the contents of the authentication demand 8311 are not changed (step S8312). Similarly, the home gateway 8102 acts to the receiving node 8101 as the forward of this (step S8313). The transmitting node 8101 interprets this as it being the authentication demand published from the home gateway 8101.

[0219] The same procedure as this is constructed bidirectionally, and authentication procedure is performed between the transmitting node 8101 and the receiving node 8104 (step S8314). In the meantime, the home gateway acts as the forward of the packet of this procedure, without changing contents. The receiving node 8104 receives a key and exchanging key information, comes to be able to perform a decryption of the enciphered MPEG 2 image after all in parallel to authentication.

[0220] A deer is carried out, the MPEG image which the transmitting node 8101 transmits is enciphered using the contents key K, and this follows the path synchronous CHIENERU#y of synchronous CHIENERU #x of 1394 buses, the home gateway 8102, a public network, the home gateway 8103, and 1394 buses, and reaches the receiving node 8103 (steps S8315-S8317). And in the receiving node 8103, using a cryptographic key K, a code decryption is carried out, the enciphered MPEG image is decoded, and it is indicated by playback.

[0221] Thus, also in the environment where a home network and the Internet

interconnected, through the home gateway which offers redundancy, it is enciphered in all the paths that it cannot copy, the required data transfer of contents protection, such as an actual MPEG image, can be performed, and safe data transfer is possible because a transmitting node and a receiving node perform authentication procedure and key exchange procedure. Thus, also in the environment of such interconnect, it becomes possible to perform data transfer in consideration of copy protection.

[0222] In addition, in the 5th operation gestalt, when the communication band of a public network is not large enough, it enables some advanced depreciation deduction to perform data transfer which took copy protection into consideration between both the home networks of a certain thing by performing coding conversion (for example, the home gateway 8102 the home gateway 8103 MPEG 2 / MPEG4 conversion, MPEG4 / MPEG 2 conversion) of the 4th operation gestalt in both the home gateway.

[0223] (6th operation gestalt) In the 1st operation gestalt, the junction node was connected with both the IEEE1394 bus and the wireless network, and the authentication and key exchange system in the case of exchanging the image data enciphered between the transmitting node on an IEEE1394 bus and the wireless node of a wireless screen oversize were explained. With the 1st operation gestalt, actual authentication and key exchange represented by exchange of an authentication format etc. are the forms where a direct deed and junction node relays these data transparent between a transmitting node and a wireless node, and this has been realized.

[0224] On the other hand, with the 6th operation gestalt, the unit of authentication and key exchange is performed like the 2nd operation gestalt, respectively between a transmitting node and a junction node and between a junction node and a wireless node. However, unlike the 2nd operation gestalt, an approach which does not have the need of performing decryption of the code of contents data and re-encryption in a junction node is explained. That is, although the procedure of having decrypted the code of the IEEE1394 section in a junction node, and enciphering the wireless section again about the data which arrived was used with the 2nd operation gestalt, it is the approach that the encryption data which arrived from the IEEE1394 bus side can be transmitted to a wireless screen oversize as it is with the 6th operation gestalt.

[0225] An example of the whole configuration of the home network of a certain home is shown in drawing 77 . This whole configuration is the same as that of the 2nd operation gestalt fundamentally.

[0226] An example of the internal structure of the transmitting node 9101 is shown in drawing 78 . The same is fundamentally [as the 2nd operation gestalt] said of this. The authentication format Acert is prepared for one node.

[0227] An example of the internal structure of the junction node 9102 is shown in drawing 79 . One (it is Ccert to Bcert and wireless network side in IEEE1394 side) preparation of the authentication formats Bcert and Ccert is carried out for every network interface. Between the ISO signal sender and receiver 9203 by the side of IEEE1394, and the wireless ISO signal sender and receiver 9206, it is the same as that of the 2nd operation gestalt except for the point that the stream signal enciphered directly (** which does not pass through the process of a decryption / re-encryption) is exchanged.

[0228] An example of the internal structure of the wireless node 9103 is shown in drawing 80 . The same is fundamentally [as the 2nd operation gestalt] said of this. The authentication format Dcert is prepared for one node.

[0229] By the junction node, it considers as the thing of service on IEEE1394 which has a substitute service function, respectively like an old operation gestalt at an IEEE1394 side at the wireless network side of service of a wireless screen oversize. In addition, detailed explanation here is omitted.

[0230] Next, the example of a sequence of this whole operation gestalt is shown in drawing 81 . The junction node is advertising in the substitute the service (image transmitting subunit) which the transmitting node offers to the wireless network side like an old operation gestalt, and a wireless node (image decoding subunit) performs an actual image transfer request to the image transmitting subunit of the transmitting node which offers a demand and service with an actual junction node for service (MPEG image transfer request) to the redundancy of a junction node. A wireless synchronous channel #y top shall be transmitted for synchronous channel #x top to a wireless screen oversize by the IEEE1394 top in the form where actual image data were enciphered. In addition, since it is the same as that of an old operation gestalt for details, detailed explanation here is omitted.

[0231] Moreover, the example of operations sequence of the junction node 9102 is shown in drawing 83 / drawing 84 , and the example of operations sequence of the wireless node 9103 is shown for the example of operations sequence of the transmitting node 9101 in drawing 82 at drawing 85 / drawing 86 , respectively.

[0232] With this operation gestalt, the procedure which applies in authentication and key exchange system of "5C Digital TransmissionContent ProtoctionSpecification" which is a protection-of-copyrights method on IEEE1394 fundamentally shall be completed. In addition, this operation gestalt explains the case where authentication and key exchange system are held per node (the 7th operation gestalt explains the case where it carries out per subunit).

[0233] Now, the transmitting node 9101 transmits the MPEG image enciphered with the contents key K on synchronous channel #x of IEEE1394 (steps S8501, S8601, and S8701). The junction node 9102 which received this is transmitted to wireless synchronous channel #y by the side of a wireless network as it is (have enciphered the received MPEG image with the contents key K) (steps S8509 and S8701).

[0234] It is recognized as the junction node 9102 recognized that the data received through synchronous channel #y are enciphered being carried out with reference to the transmitting node ID field (SID field) of the CIP header of data which arrived etc., and carrying out authentication and key exchange with the transmitting node 9101 (step S8801). An authentication demand packet including the authentication format Bcert of the junction node 9102 is transmitted to the transmitting node 9101 (steps S8502 and S8702).

[0235] The transmitting node 9101 which received this transmits an authentication demand packet including the authentication format Acert of a transmitting node to the junction node 9102 (steps S8503, S8602, S8603, and S8703).

[0236] Next, authentication and key exchange procedure are performed and the authentication key Kauth1 is shared between both transmitting node 9101 and junction node 9102 in secrecy (steps S8504, S8505, S8604, and S8704).

[0237] In an IEEE1394 protection-of-copyrights method, the contents key K is calculated with the function J of three variables, the exchange key Kx, Seed Nc, and the code control information EMI. That is, it is K=J (Kx, Nc, EMI). EMI is a value surely given to the encryption data transmitted here. therefore, the transmitting node 9101 needs to notify the value of the exchange key Kx and Seed Nc also for a wireless node the case of a junction node and this operation gestalt ·· to a receiving side.

[0238] Then, the transmitting node 9101 transmits to the junction node 9102 in the form of f (Kx, Kauth) using the known function f using the authentication key Kauth1 shared between the junction nodes 9102 (steps S8506, S8605, S8708, and S8709). The junction node 9102 can compute the value of Kx from this value. Similarly, Seed's Nc value is also transmitted to the junction node 9102 from the transmitting node 9101 (steps S8507, S8606, and S8710). It means that the junction node 9102 had recognized the value of Kx required to generate the contents key K which decodes a code, and Nc here at this time.

[0239] Now, same procedure is performed also between the junction node 9102 and the wireless node 9103 (step S8510· S8513, S8705-S8707, S8802-S8804). Since this procedure is the same as the authentication and key exchange procedure between the transmitting node 9101 and the junction node 9102, detailed explanation here is

omitted. Here, the address information which can identify the junction node 9102 which is a transmitting agency node may also be given to the enciphered data to which the wireless synchronous channel #y top of a wireless network is transmitted.

[0240] Now, the authentication key Kauth2 should be sharable by the junction node 9102 and the wireless node 9101. With this operation gestalt, in order for the junction node 9102 to perform forward processing on a wireless network (wireless synchronous channel #y) as it is, without decrypting a code for the enciphered MPEG image, the junction node 9102 needs to notify the value of the same exchange key Kx as the IEEE1394 section, and Seed Nc to the wireless node 9103 (if it can notify conversely, a decryption of a code is possible for the wireless node 9103.). However, the IEEE1394 section and the wireless network section shall be managed by the same contents protection policy. Then, the junction node 9102 transmits similarly each value of Kx and Nc which were computed from the data received by S8506 and S8507 to the wireless node 9103 (steps S8514, S8515, S8709, S8711, S8805-S8807). Specifically the value of Kx calculates f (Kx, Kauth2) using the value of the authentication key Kauth2, and sends it out to the wireless node 9103, and the value of Nc is transmitted as it is.

[0241] In the wireless node 9103, since the value of Kx and Nc can be recognized using the same procedure as a junction node, the value of the contents key K is computable using the same function J (step S8516).

[0242] Therefore, the MPEG image enciphered with the contents key K sent from the transmitting node 9101 Even when a decryption of a code is not made, but it acts as a forward as it was and it has been transmitted to the wireless node 9103 by the junction node 9102 (steps S8508, S8517, S8607, S8712, and S8809) A decryption of a code can be performed using the value of the contents key K previously calculated by S8516 (steps S8518 and S8810). Then, decoding of an MPEG image, a display display, etc. are performed.

[0243] In addition, although this operation gestalt has explained noting that the wireless synchronous channel is defined by the wireless screen oversize and this wireless synchronous channel top is transmitted to the enciphered MPEG image Like the 2nd operation gestalt, also when transmitting the wireless frame as Ethernet with the same QOS data transfer in a wireless screen oversize, the same approach (it acts to a wireless node as the forward of the value of Kx and Nc from a junction node) can be applied.

[0244] Conversely, if it says, construction of a low cost junction node will be attained from a decryption and re-encryption of a code becoming unnecessary in the junction node 9102, and a high-speed packet transfer being attained by approach like this

operation gestalt.

[0245] In addition, node (another node) with the another transmitting node 9102 exists in the IEEE1394 side in this case, and the data (data which had the same EMI strictly) enciphered by the wireless node 9103 with another contents key through the junction node 9102 from this another node cannot be transmitted. Since the contents key serves as structure which the transmitting node 9101 of data determines fundamentally, there is possibility of enough that another node will choose another contents key. However, the contents key K is already defined as a meaning between the junction node 9102 and the wireless node 9103. That is, between the junction node 9102 and the wireless node 9103, only one contents key is sharable about the same EMI value. Therefore, among both nodes, since another contents key cannot be generated in case this is transmitted to the wireless node 9103 from the junction node 9102 even if it receives the data (enciphered with another contents key) from another node, since only at most one contents key can be used, this can be decrypted.

[0246] Therefore, the junction node 9102 becomes possible [avoiding the above-mentioned conflict beforehand] by refusing this, when there is a Request to Send of encryption data with the need of using another contents key, to the node (in the case of this operation gestalt wireless node 9103) which has already transmitted encryption data (for example, when there is a service request to substitute service of another node of IEEE1394 etc.). moreover -- the case where the junction node 9102 has already transmitted encryption data to the wireless node 9103 -- this wireless node 9103 -- receiving -- other services (subunit) -- not showing (the substitute service provision itself being interrupted or offer of the substitute service accompanied by an encryption stream transmission being interrupted **) -- the same effectiveness can be considered also in the way to say.

[0247] (7th operation gestalt) It was the approach which does not have the need that perform the unit of authentication and key exchange, respectively between a transmitting node and a junction node and between a junction node and a wireless node, and a junction node performs decryption of a code, and re-encryption with the 6th operation gestalt.

[0248] On the other hand, with the 7th operation gestalt, although the thing without the need of performing decryption of a code and re-encryption in a junction node is the same, it is a case so that the unit of the authentication and key exchange by the side of a wireless network may be made per subunit as well as the 2nd operation gestalt and can have two or more contents keys also between the same nodes. According to this operation gestalt, coincidence reception of the encryption data from two or more

transmitting node on IEEE1394 is attained.

[0249] An example of the whole configuration of the home network of a certain home is shown in drawing 87 . This whole configuration is the same as that of the 6th operation gestalt fundamentally except a point with two transmitting nodes (P and Q).

[0250] The internal configuration of the transmitting nodes 9801 and 9811 is the same as that of the 6th operation gestalt.

[0251] In an IEEE1394 side, the unit of authentication and key exchange is between nodes, and the internal configuration of the junction node 9802 is the same as that of the 6th operation gestalt at a wireless network side except for the point that the unit of authentication and key exchange is between subunits.

[0252] The internal configuration of the wireless node 9803 is the same as that of the 6th operation gestalt except for the point that the unit of authentication and key exchange is between subunits.

[0253] In addition, the operations sequence of the transmitting nodes 9801 and 9811 and the wireless node 9802 is the same as that of the 6th operation gestalt fundamentally. Moreover, the operations sequence of the junction node 9803 in the case of acting as intermediary to one transmitting node is the same as that of the 6th operation gestalt fundamentally.

[0254] By the junction node, it considers as the thing of service on IEEE1394 which has a substitute service function, respectively like an old operation gestalt at an IEEE1394 side at the wireless network side of service of a wireless screen oversize. In addition, detailed explanation here is omitted.

[0255] Next, the example of operations sequence of the junction node 9802 in the case of acting as intermediary to two or more transmitting nodes is shown in drawing 88 , and the example of a sequence of this whole operation gestalt is shown in drawing 89 / drawing 90 . The junction node is advertising in the substitute the service (image transmitting subunit) which the transmitting node offers to the wireless network side like an old operation gestalt, and a wireless node (image decoding subunit) performs an actual image transfer request to the image transmitting subunit of the transmitting node which offers a demand and service with an actual junction node for service (MPEG image transfer request) to the redundancy of a junction node. A wireless synchronous channel #y top shall be transmitted for synchronous channel #x top to a wireless screen oversize by the IEEE1394 top in the form where actual image data were enciphered. Since it is the same as that of an old operation gestalt for details, detailed explanation here is omitted.

[0256] The procedure which applies in authentication and key exchange system of "5C

Digital Transmission Content ProtoctionSpecification" which is a protection-of-copyrights method on IEEE1394 fundamentally also with this operation gestalt shall be completed.

[0257] Now, the transmitting node P (9801) transmits the MPEG image enciphered with the contents key K1 on synchronous channel #x of IEEE1394 (steps S9201 and S9301). The contents key K1 shall be calculated in K1=J (Kxp, Ncp, EMI) like the 6th operation gestalt. The junction node 9802 which received this is transmitted to wireless synchronous channel #y by the side of a wireless network as it is (have enciphered the received MPEG image with the contents key K1) (steps S9209 and S9301).

[0258] Since the procedure (step S9202- S9207, S9302) in which the junction node 9802 carries out an authentication demand to the transmitting node P, performs key exchange etc., and gains the exchange key Kxp and Seed Ncp is the same as that of the 6th operation gestalt, detailed explanation here is omitted. It means that the junction node 9802 had recognized the value of KxpNcp required in order to decode a code at this time.

[0259] Now, same authentication and key exchange procedure are performed also between the junction node 9802 and the wireless node 9803 (step S9210- S9217, S9303). Since this procedure is the same as the authentication and key exchange procedure between the transmitting node of the 2nd operation gestalt, and a junction node, detailed explanation here is omitted. However, the identifier of a plug which will perform transmission and reception of others, a channel number, or encryption data to an authentication place inquiry, an authentication place response, or an authentication demand may be carried, and this may be performed. [ID / of a subunit] Even if it is the authentication and key exchange between the same nodes, about the encryption data of a different key, it becomes possible to notify a different key, so that the junction node 9802 or the wireless node 9803 can identify now "the authentication and key exchange procedure it is" and it may be mentioned later. [about which encryption data]

[0260] In addition, when including a channel number in an authentication demand in this case, the authentication place response of an authentication place inquiry of step S9210 and step S9211 becomes unnecessary.

[0261] Now, the authentication key Kauth1 should be sharable by the junction node 9802 and the wireless node 9803. Also with this operation gestalt, in order for the junction node 9802 to perform forward processing on a wireless network (wireless synchronous channel #y) as it is, without decrypting a code for the enciphered MPEG image, the junction node 9802 needs to notify the value of the exchange key Kxp and Seed Ncp to the wireless node 9803 (if it can notify conversely, a decryption of a code is

possible for the wireless node 9803). Then, the junction node 9802 transmits similarly each value of Kxp and Ncp which were computed from the data received by S9206 and S9207 to the wireless node 9803 (steps S9216 and S9217). The value of Kxp calculates f (Kxp, Kauth1) using the value of the authentication key Kauth1, and sends it out to the wireless node 9803 (step S9216).

[0262] In the wireless node 9803, since the value of Kxp and Ncp can be recognized using the same procedure as the junction node 9802, the value of the contents key K1 is computable using the same function J (step S9218).

[0263] Therefore, even when it acts as the forward of the MPEG image enciphered with the contents key K1 sent from the transmitting node P as it was and has been transmitted to the wireless node 9803 by the junction node 9802, without decrypting a code (steps S9208 and S9219), a decryption of a code can do it using the value of the contents key K1 previously calculated at step S9218 (step S9220). Then, decoding of an MPEG image, a display display, etc. are performed.

[0264] Construction of a low cost junction node is attained from a decryption of a code and re-encryption becoming unnecessary in the junction node 9802, and a high-speed packet transfer being attained also by approach like this operation gestalt.

[0265] Now, the case (steps S9221, S9229, and S9304) where the data as which another transmitting node Q (9811) was enciphered by coincidence with another contents key K2 to the wireless node 9803 next through the junction node 9802 are transmitted is considered.

[0266] Like the first half of this operation gestalt, authentication and key exchange are performed between the transmitting node Q and the junction node 9802 (steps S9222-S9227), and the junction node 9802 can acquire the value of the exchange key Kxq and Seed Ncq, respectively.

[0267] In this operation gestalt, since the authentication between the junction node 9802 and the wireless node 9803 is a unit between subunits, two or more authentication and key exchange between the thing currently performed between the subunits from which transmission and reception of encryption data differ, then the junction nodes 9802 and the wireless nodes 9803 of it are attained.

[0268] That is, authentication and key exchange are performed like the first half of this operation gestalt between different subunits from the first half of this operation gestalt between the junction node 9802 and the wireless node 9803 (step S9230- S9235, S9305). Moreover, the junction node 9802 acts to the exchange key Kxq between the transmitting node Q and the self-node (junction node) 9802 as the forward of the seed Ncq at the wireless node 9803 (steps S9236, S9237, S9305, and S9306).

[0269] In the wireless node 9803, since the value of Kxq and Ncq can be recognized, the value of the contents key K2 is computable using the same function J (step S9238).

[0270] Therefore, even when it acts as the forward of the MPEG image enciphered with the contents key K2 sent from the transmitting node Q as it was and has been transmitted to the wireless node 9803 by the junction node 9802, without decrypting a code (steps S9228 and S9229), a decryption of a code can do it using the value of the contents key K2 previously calculated at step S9238 (step S9240). That is, coincidence reception of the MPEG image enciphered with two different contents keys (it is K1 and K2 at this operation gestalt) is attained.

[0271] In addition, although the 6th operation gestalt and the 7th operation gestalt have explained the case where interconnect with IEEE1394 and a wireless network is performed to the example, it is applicable also about the network of others, such as the Internet.

[0272] in addition, the 1· this invention can be applied also when carrying out data transfer in the direction contrary to the direction of the data transfer illustrated in the 7th operation gestalt (for example, when carrying out data transfer from a wireless node to the node on IEEE1394).

[0273] moreover, the 1· in the 7th operation gestalt, although the wireless node and the node on IEEE1394 were explained about contents paying attention to either the transmitting function or the reception function, a wireless node and the node on IEEE1394 can also have both a transmitting function and a reception function about contents

[0274] Moreover, neither authentication procedure nor key exchange procedure (contents key share procedure) is limited to what was illustrated until now, but also when other various approaches are used, it can apply this invention.

[0275] Moreover, above, although the operation gestalt was explained as a home network network, of course, this invention is applicable also to networks other than a home network.

[0276] In addition, each above function is realizable also as software.

[0277] Moreover, this operation gestalt can also be carried out also as a record medium which recorded the program (or in order to operate a computer as a predetermined means, or in order to make a computer realize a predetermined function) for performing a predetermined means on the computer and in which computer read is possible.

[0278] This invention is not limited to the gestalt of operation mentioned above, in the technical range, can deform variously and can be carried out.

[0279]

[Effect of the Invention] According to this invention, it becomes possible to perform contents protection procedure for transmission and reception of the contents which should be protected between the equipment which is not connected in the same network.

[Translation done.]

CLAIMS

[Claim(s)]

[Claim 1] The 1st interface means connected to the 1st network, and the 2nd interface means connected to the 2nd network, A substitute configuration means to indicate the equipment on said 2nd network, service, or a subunit to said 1st network side as a thing on self-repeating installation, A control command receiving means to receive this equipment, service, or the control command signal addressed to a subunit from said 1st network side, A control command transmitting means to transmit the signal corresponding to said control command signal received with this control command receiving means to the equipment on said 2nd network, service, or a subunit, A contents protection information receiving means to receive said equipment, the service, or the contents protection information addressed to a subunit disclosed with said substitute configuration means from the equipment on said 1st network, Repeating installation characterized by providing a contents protection information transfer means not to add modification to the contents protection information received with this contents protection information receiving means, but to transmit to the equipment on said 2nd network, service, or a subunit.

[Claim 2] The 1st interface means connected to the 1st network, and the 2nd interface means connected to the 2nd network, A substitute configuration means to indicate respectively the equipment on the 1st and 2nd networks, service, or a subunit to the network side of another side as a thing on self-repeating installation, A control command receiving means to receive this equipment, service, or the control command signal addressed to a subunit from the network side indicated with said substitute configuration means, A control command transmitting means to transmit the signal corresponding to said control command signal received with this control command receiving means to the equipment on the network indicated with said substitute configuration means, and a different network, service, or a subunit, A contents

protection information receiving means to receive said equipment, the service, or the contents protection information addressed to a subunit disclosed with said substitute configuration means from the equipment on said 1st or 2nd network, A contents protection information transfer means not to add modification to the contents protection information received with this contents protection information receiving means, but to transmit to the equipment on the network of said another side, service, or a subunit, It is said equipment, the service, or addressing to a subunit indicated with said substitute configuration means from the equipment on said 1st or 2nd network. A contents receiving means to receive the contents protected with the contents key obtained from said contents protection information, Repeating installation characterized by providing a contents transfer means not to add modification to said contents which received with this contents receiving means, but to transmit to the equipment on the network of said another side, service, or a subunit.

[Claim 3] said contents protection information -- the authentication between the equipment on said 1st network, service or a subunit, and the equipment on said 2nd network, service or a subunit -- and -- or the repeating installation according to claim 2 characterized by being the information about the procedure of the contents protection including key exchange.

[Claim 4] The 1st interface means connected to the 1st network, and the 2nd interface means connected to the 2nd network, A substitute configuration means to indicate respectively the equipment on the 1st and 2nd networks, service, or a subunit to the network side of another side as a thing on self-repeating installation, A control command receiving means to receive this equipment, service, or the control command signal addressed to a subunit from the network side indicated with said substitute configuration means, A control command transmitting means to transmit the signal corresponding to said control command signal received with this control command receiving means to the equipment on the network indicated with said substitute configuration means, and a different network, service, or a subunit, Between self-repeating installation with the equipment on said 1st network, service, or a subunit Between self-repeating installation with the 1st contents safeguard which takes the necessary procedure for contents protection, and the equipment on said 2nd network, service or a subunit From the equipment on the 2nd contents safeguard which takes the necessary procedure for contents protection, and said network of either the 1st or a 2nd A contents receiving means to be the equipment on the self-repeating installation indicated with said substitute configuration means, service, or addressing to a subunit, and to receive the contents enciphered based on said contents safeguard of either the

1st or a 2nd, The contents which received with said contents receiving means are enciphered based on the contents safeguard of said 1st or 2nd any or another side. Said 1st [the] or the 2nd are the repeating installation characterized by providing a contents transmitting means to transmit to the equipment on the network of another side, service, or a subunit either.

[Claim 5] The cipher system used by said 1st contents safeguard and said 2nd contents safeguard is repeating installation according to claim 4 characterized by being a thing based on key information which is a different method or is different.

[Claim 6] Said contents receiving means and said contents transmitting means are repeating installation according to claim 4 characterized by carrying out the closure to the same LSI.

[Claim 7] Repeating installation according to claim 4 characterized by making into the same thing 1st key information used in the procedure of said contents protection in said 1st contents safeguard, and 2nd key information used in the procedure of said contents protection in said 2nd contents safeguard.

[Claim 8] Said 1st [the] or the 2nd are the repeating installation according to claim 7 characterized by performing procedure of said contents protection in the contents safeguard of another side per a contents unit, a service unit, or subunit using predetermined key information either.

[Claim 9] Repeating installation according to claim 2 or 4 characterized by to provide further a configuration information receiving means to receive the configuration information containing the existence of an authentication format of this equipment from the equipment on said 1st and 2nd networks, service, or a subunit, and a configuration recognition means to perform this equipment, service, or configuration recognition of a subunit based on each configuration information which received with said configuration information receiving means.

[Claim 10] Between self-repeating installation with the 1st interface means connected to the 1st network, the 2nd interface means connected to the 2nd network, and the equipment on said 1st network, service or a subunit Between self-repeating installation with the 1st contents safeguard which takes the necessary procedure for contents protection, and the equipment on said 2nd network, service or a subunit From the equipment on the 2nd contents safeguard which takes the necessary procedure for contents protection, and said network of either the 1st or a 2nd A contents receiving means to be the equipment on self-repeating installation, service, or addressing to a subunit, and to receive the contents enciphered based on said contents safeguard of either the 1st or a 2nd, The contents which received with said contents receiving means

are enciphered based on the contents safeguard of said 1st or 2nd any or another side. A contents transmitting means to transmit to the equipment on the network of said 1st or 2nd any or another side, service, or a subunit is provided. Repeating installation characterized by making into the same thing 1st key information used in the procedure of said contents protection in said 1st contents safeguard, and 2nd key information used in the procedure of said contents protection in said 2nd contents safeguard.

[Claim 11] Between the interface means connected to the network, and other equipments on said network, service or a subunit at least -- authentication procedure -- and -- or with a copy protection processing means to perform predetermined contents protection procedure including key exchange procedure The enciphered contents which gave the address of a self-communication device to other equipments on said network An identifiable identifier is further given to a meaning for the address and these contents of a self-communication device through a network virtual channel top. From a contents transmitting means to transmit, and other equipments on said network A receiving means to receive the inquiry about the service or the subunit which gave said identifier through said virtual channel top, and has transmitted said enciphered contents, or a plug, The communication device characterized by answering this inquiry and providing the notice means which gives the notice about the corresponding service, a subunit, or a plug to other equipments on said network.

[Claim 12] Between the interface means connected to the network, and other equipments on said network, service or a subunit at least -- authentication procedure -- and -- or with a copy protection processing means to perform predetermined contents protection procedure including key exchange procedure From other equipments on said network, the enciphered contents to which the address of other equipments on this network was given In the form where these contents were given to the identifiable identifier by the meaning, other equipments on this network through a network virtual channel top As opposed to a contents receiving means to receive, and other equipments on said network A transmitting means to transmit the inquiry about the service or the subunit which gave said identifier through said virtual channel, and has transmitted said enciphered contents, or a plug, The communication device characterized by providing a receiving means to receive the notice about the service applicable to said inquiry, a subunit, or a plug from other equipments on said network.

[Claim 13] As opposed to the interface means connected to the network, and other equipments on said network the enciphered contents between a contents transfer means to transmit or receive through the flow of the transmitting address, a transmit port, the receiving address, and a receive port constructed, come out of and identified,

and other equipments on said network Or a copy protection processing means to perform predetermined contents protection procedure including key exchange procedure is provided. the logical port appointed beforehand -- using -- at least -- authentication procedure -- and -- The communication device characterized by performing this in the unit of said flow when performing said predetermined contents protection procedure.

[Claim 14] The communication device according to claim 21 characterized by giving the identifier of said flow to the information which sets for the procedure of at least a part included in said predetermined contents protection procedure, and is made it.

[Claim 15] Between the interface means connected to the network, and other equipments on said network, service or a subunit at least -- authentication procedure -- and -- or with a copy protection processing means to perform predetermined contents protection procedure including key exchange procedure The enciphered contents to which the address of the equipment of a transmitting side was given to other equipments on said network In the form to which the identifiable identifier was given by the meaning, the equipment of this transmitting side these contents through a network virtual channel top To the information which sets for the procedure of at least a part which possesses a contents transceiver means to transmit or receive, and is included in said predetermined contents protection procedure, and is made it The communication device characterized by the service and the subunit which exchange said enciphered contents, a virtual channel, the identifier of a plug, or the equipment of said transmitting side giving at least one of identifiable identifiers to a meaning for said contents.

[Claim 16] The 1st interface means connected to the 1st network, and the 2nd interface means connected to the 2nd network, The equipment, the service, or the subunit on the 1st network, at least -- authentication procedure -- and -- or with the copy protection processing means of predetermined contents protection procedure ****** 1 including key exchange procedure The equipment, the service, or the subunit on the 2nd network, at least -- authentication procedure -- and -- or with the copy protection processing means of the predetermined contents protection procedure 2nd including key exchange procedure A contents receiving means to receive the data containing the specific contents enciphered from said 1st interface means, A decryption means to decrypt said enciphered data which were received from said 1st interface means with the key for contents protection for which it is provided with said 1st copy protection processing means, A conversion means to change said decrypted data into the data of another coding format, An encryption means to encipher said decrypted data with the key for

contents protection for which it is provided with said 2nd copy protection processing means, Repeating installation characterized by providing a contents transmitting means to transmit said enciphered data to said 2nd interface means.

[Claim 17] As a thing on self-repeating installation, while indicating the equipment on said 2nd network, service, or a subunit to said 1st network side When the information addressed to the equipment indicated as a thing on self-repeating installation, service, or a subunit is received from the equipment by the side of said 1st network While transmitting the information on the contents according to this information to the equipment on said 2nd network, service, or a subunit As a thing on self-repeating installation, while indicating the equipment on said 1st network, service, or a subunit to said 2nd network side When the information addressed to the equipment indicated as a thing on self-repeating installation, service, or a subunit is received from the equipment by the side of said 2nd network A substitute configuration means to transmit the information on the contents according to this information to the equipment on said 1st network, service, or a subunit is provided further. Said substitute configuration means The equipment on one [said] 1st or 2nd network, the equipment on the network of said 1st or 2nd another side, service, or a subunit, at least -- authentication procedure -- and -- or, in performing predetermined contents protection procedure including key exchange procedure While performing the equipment on one [said] network, and this predetermined contents protection procedure using one [said] 1st or 2nd copy protection processing means Repeating installation according to claim 24 characterized by performing the equipment on the network of said another side, service or a subunit, and this predetermined contents protection procedure using the copy protection processing means of said 1st or 2nd another side.

[Translation done.]

MB/DN/P0410

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－174797
（P2000－174797A）
(43)公開日　平成12年６月23日(2000.6.23)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　11/00	３１０Ｃ	
12/28		Ｇ１１Ｂ　20/10	Ｈ	
Ｇ１１Ｂ　20/10		Ｈ０４Ｌ　9/00	６７３Ａ	
Ｈ０４Ｌ　9/32			６７５Ｄ	
12/66		11/20	Ｂ	

審査請求　未請求　請求項の数17　ＯＬ　（全 60 頁）　最終頁に続く

(21)出願番号　特願平11－209836

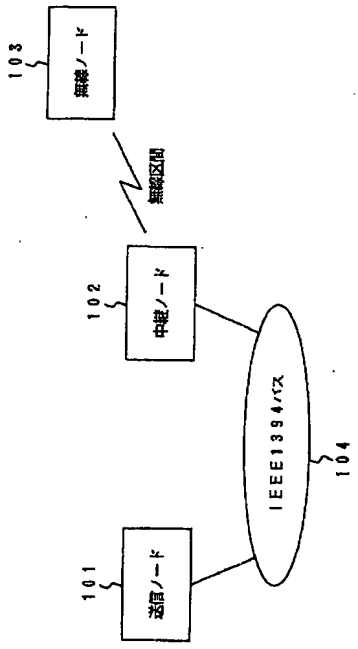
(22)出願日　平成11年７月23日(1999.7.23)

(31)優先権主張番号　特願平10－292824
(32)優先日　平成10年９月30日(1998.9.30)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　斉藤　健
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　高畠　由彰
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　中継装置及び通信装置

(57)【要約】
【課題】　同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置を提供すること。
【解決手段】　第１のネットワーク１０４と第２のネットワークに接続され、第２のネットワーク上の装置１０３を自中継装置１０２上のものとして第１のネットワーク１０４側に開示する機能と、第１のネットワーク１０４上の装置１０１から装置１０３宛の制御コマンドを受信した場合、これに対応する制御コマンドを装置１０３へ送信する機能と、装置１０１から装置１０３宛のコンテンツ保護情報を受信した場合、これに変更を加えずに装置１０３へ送信する機能と、装置１０１から装置１０３宛に先のコンテンツ保護情報から得られるコンテンツ鍵で保護されたコンテンツを受信した場合、これに変更を加えずに装置１０３へ送信する機能とを有する。



1

【特許請求の範囲】

【請求項１】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして前記第１のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第１のネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を前記第２のネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記第２のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段とを具備したことを特徴とする中継装置。

【請求項２】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、

このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段と、

前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られる

2

コンテンツ鍵で保護されたコンテンツを受信するコンテンツ受信手段と、

このコンテンツ受信手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ転送手段とを具備したことを特徴とする中継装置。

【請求項３】前記コンテンツ保護情報は、前記第１のネットワーク上の装置又はサービス又はサブユニットと、前記第２のネットワーク上の装置又はサービス又はサブユニット間の認証及び又は鍵交換を含むコンテンツ保護の手続きに関する情報であることを特徴とする請求項２に記載の中継装置。

【請求項４】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、

この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、

この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、

前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、

前記第１又は第２のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項５】前記第１のコンテンツ保護手段と、前記第２のコンテンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる鍵情報に基づくものであることを特徴とする請求項４に記載の中継装置。

【請求項６】前記コンテンツ受信手段と、前記コンテン

ツ送信手段は同一のＬＳＩに封止されていることを特徴とする請求項４に記載の中継装置。

【請求項７】前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとすることを特徴とする請求項４に記載の中継装置。

【請求項８】前記第１又は第２のいずれか他方のコンテンツ保護手段における前記コンテンツ保護の手続きは、所定の鍵情報を用いて、コンテンツ単位又はサービス単位又はサブユニット単位で行なうことを特徴とする請求項７に記載の中継装置。

【請求項９】前記第１及び第２のネットワーク上の装置又はサービス又はサブユニットから、該装置の認証フォーマットの有無を含む構成情報を受信する構成情報受信手段と、

前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサービス又はサブユニットの構成認識を行う構成認識手段とを更に具備したことを特徴とする請求項２または４に記載の中継装置。

【請求項１０】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、

前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、

前記第１又は第２のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、

前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備し、

前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとすることを特徴とする中継装置。

【請求項１１】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、

前記ネットワーク上の他の装置から、前記仮想チャネル上を介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはブラグについての問合せを受信する受信手段と、

この問合せに応答して、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはブラグについての通知をする通知手段とを具備することを特徴とする通信装置。

【請求項１２】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、

前記ネットワーク上の他の装置に対して、前記仮想チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはブラグについての問合せを送信する送信手段と、

前記ネットワーク上の他の装置から、前記問合せに該当するサービスまたはサブユニットまたはブラグについての通知を受信する受信手段とを具備することを特徴とする通信装置。

【請求項１３】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフローを介して送信または受信するコンテンツ転送手段と、

前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段とを具備し、

前記所定のコンテンツ保護手続きを行なう場合には、これを前記フローの単位で行なうことを特徴とする通信装置。

【請求項１４】前記所定のコンテンツ保護手続きに含ま

れる少なくとも一部の手続きにおいてやり取りされる情報に前記フローの識別子を付与することを特徴とする請求項２１に記載の通信装置。

【請求項１５】ネットワークに接続されたインタフェース手段と、

前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、

前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、

前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサービス、サブユニット、仮想チャネルもしくはプラグの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子のうちの少なくとも一つを付与することを特徴とする通信装置。

【請求項１６】第１のネットワークに接続された第１のインタフェース手段と、

第２のネットワークに接続された第２のインタフェース手段と、

第１のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き行う第１のコピープロテクション処理手段と、

第２のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き第２のコピープロテクション処理手段と、

前記第１のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第１のインタフェース手段から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、

前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、

前記復号化されたデータを、前記第２のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、

前記暗号化されたデータを、前記第２のインタフェース手段へ転送するコンテンツ送信手段とを具備したことを特徴とする中継装置。

【請求項１７】前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示するとともに、前記第１のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第２のネットワーク上の装置またはサービスまたはサブユニット宛に送信するとともに、

前記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示するとともに、前記第２のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第１のネットワーク上の装置またはサービスまたはサブユニット宛に送信する代理構成手段を更に具備し、

前記代理構成手段は、前記第１または第２の一方のネットワーク上の装置と、前記第１または第２の他方のネットワーク上の装置またはサービスまたはサブユニットとの、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１または第２の一方のコピープロテクション処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第１または第２の他方のコピープロテクション処理手段を用いて前記他方のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うことを特徴とする請求項２４に記載の中継装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＩＥＥＥ１３９４バスや無線ネットワーク等のネットワーク間のデータ転送を中継する中継装置及びＩＥＥＥ１３９４バスや無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

【０００２】

【従来の技術】近年、デジタル放送の開始や、デジタルＡＶ機器の発売等、いわゆる「家庭ＡＶ環境のデジタル化」が大きな注目を集めている。デジタルＡＶデータは、様々な圧縮が可能、マルチメディアデータとしても処理が可能、何回再生しても劣化がない、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

【０００３】しかしながら、このデジタルＡＶ技術には、反面、「コンテンツの不正コピーが容易に行える」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビットのコピー」で、元どおりの品質の、しかも未来永劫にわたって一切劣化のない複製が作れてしまうため、いわゆる「不正コピー」の問題が発生する。

【０００４】この「不正コピー」を防ぐための技術がい

くつか検討されている。その中の一つが、ＣＰＴＷＧ（コピープロテクション技術ワーキンググループ）で検討されている「１３９４ＣＰコンテンツ保護システム仕様（１３９４ＣＰ Ｃｏｎｔｅｎｔ Ｐｒｏｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ Ｓｐｅｃｉｆｉｃａｔｉｏｎ）」である。この技術は、ＩＥＥＥ１３９４バスに接続されたノード間で、転送するコンテンツ（例えばＭＰＥＧデータ等）について、送受信ノードの間で予め認証手続きを行い、暗号鍵（コンテンツキー）を共有できるようにしておき、以降は転送するコンテンツを暗号化して転送し、認証手続きを行った両者以外はコンテンツが読めないようにする技術である。このようにすることにより、認証手続きを行っていないノードは、コンテンツキーの値がわからないため、転送されているデータ（暗号化されているデータ）をたとえ取り込むことができたとしても、この暗号を復号化することはできない。このような認証に参加できるノードは、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、不正コピーを予め防ぐことが可能になる。

【０００５】

【発明が解決しようとする課題】ＩＥＥＥ１３９４バスは、最低速度でも１００Ｍｂｐｓ、網そのものに自動構成認識機能が備わっている、ＱＯＳ転送機能を持つ等、非常に優れた特徴を持つネットワークシステムであり、それゆえに家庭向けのデジタルＡＶ向けのネットワークとして、デファクトスタンダードの地位を築いている。

【０００６】しかし、ＩＥＥＥ１３９４は、これら特徴のゆえに、「ＩＥＥＥ１３９４と、他のネットワークを接続するとき」に様々な制約を生んでいる。例えば、無線網や公衆網とＩＥＥＥ１３９４バスを接続する場合は、これらの網が１００Ｍｂｐｓ以上といった高速性を一般には有していないことや、ＩＥＥＥ１３９４の自動構成認識機能をこれらの網へそのまま拡張する、といった方法が簡単にはとれないことから、ＩＥＥＥ１３９４プロトコルをそのまま無線や公衆網に拡張する、といった方法を使うことはできない。そこで、ＩＥＥＥ１３９４と、無線網や公衆網などの他網の間にプロトコル変換ゲートウェイを配置し、相互接続する方法や、片方の網上のサービスをもう片方の網のサービスとして提供するいわゆる代理サーバの方法等が提案されている。

【０００７】これらの方法を、従来の技術で述べた１３９４コピープロテクションに適用しようとした場合、現状では該コピープロテクション技術がＩＥＥＥ１３９４バスについてのみ定められている状況である。このコピープロテクション技術を「ＩＥＥＥ１３９４と、他のネットワークを接続するとき」に拡張するための技術はないのが現状である。

【０００８】本発明は、上記事情を考慮してなされたもので、コピープロテクション技術をＩＥＥＥ１３９４のみならず、これと相互接続された他網にも拡張可能な中継装置及び通信装置を提供することを目的とする。

【０００９】また、本発明は、同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置及び通信装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】本発明（請求項１）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、前記第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして前記第１のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記第１のネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を前記第２のネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第１のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記第２のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段とを具備したことを特徴とする。

【００１１】本発明（請求項２）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛のコンテンツ保護情報を受信するコンテンツ保護情報受信手段と、このコンテンツ保護情報受信手段で受信したコンテンツ保護情報に変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ保護情報転送手段と、前記第１又は第２のネットワーク上の装置から、前記代理構成手段で開示した前記装置又はサービス又はサブユニット宛であり、前記コンテンツ保護情報から得られるコンテンツ鍵で保護

されたコンテンツを受信するコンテンツ受信手段と、このコンテンツ受信手段で受信した前記コンテンツに変更を加えず、前記他方のネットワーク上の装置又はサービス又はサブユニット宛に転送するコンテンツ転送手段とを具備したことを特徴とする。

【００１２】好ましくは、前記コンテンツ保護情報は、前記第１のネットワーク上の装置又はサービス又はサブユニットと、前記第２のネットワーク上の装置又はサービス又はサブユニット間の認証及び又は鍵交換を含むコンテンツ保護の手続きに関する情報であるようにしてもよい。

【００１３】本発明によれば、例えば、保護すべきコンテンツの送信もしくは受信を行っているペアである「代理構成手段が提供している第２のネットワーク上の装置またはサービスまたはサブユニット（以下、装置またはサービスまたはサブユニットを装置等と呼ぶ）」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「代理構成手段が提供している第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がその手続きを中身を変えることなく中継することによって、そのコンテンツ保護手続きを直接「代理構成手段が提供している第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において行うことができる。

【００１４】また、本発明によれば、保護されるべきコンテンツを、その保護形式を変更することなく受信側に送り届けることができ、コンテンツを保護された形でエンドエンドに送り届けることができる。

【００１５】本発明（請求項４）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、第１及び第２のネットワーク上の装置又はサービス又はサブユニットを、自中継装置上のものとして各々他方のネットワーク側に開示する代理構成手段と、この装置又はサービス又はサブユニット宛の制御コマンド信号を前記代理構成手段で開示したネットワーク側から受信する制御コマンド受信手段と、この制御コマンド受信手段で受信した前記制御コマンド信号に対応した信号を、前記代理構成手段で開示したネットワークと異なるネットワーク上の装置又はサービス又はサブユニット宛に送信する制御コマンド送信手段と、前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、前記第１又は第２のいずれか一方のネットワーク上の装置から、前記代理構成手段で開示した自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備したことを特徴とする。

【００１６】本発明によれば、例えば、保護すべきコンテンツの送信もしくは受信を行っているペアである「第２のネットワーク上の装置等」と「第１のネットワーク上の装置」との間において、「第１のネットワーク上の装置」または「第２のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第１のネットワーク上の装置」または「第２のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、例えば、中継装置が、コンテンツ保護手続きをそれぞれ終端することで、結局、「第２のネットワーク上の装置等」と中継装置との間、および中継装置と「第１のネットワーク上の装置」との間で、コンテンツ保護手続きをそれぞれ行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【００１７】また、第１のネットワーク上の装置から第２のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、不正コピー等を未然に防ぐことが可能になる。

【００１８】好ましくは、前記第１のコンテンツ保護手段と、前記第２のコンテンツ保護手段で用いられる暗号化方式は異なる方式であるか、又は異なる鍵情報に基づくものであるようにしてもよい。

【００１９】好ましくは、前記コンテンツ受信手段と、前記コンテンツ送信手段は同一のＬＳＩに封止されているようにしてもよい。これによって、この復号化手段と暗号化手段との間は、暗号化されていないコンテンツデータが流れるため、個々にプローブをあてる等して、ここからコンテンツデータを盗聴し、不正コピーを働くことを未然に防止することが可能となる。

【００２０】好ましくは、前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとするようにしてもよい。これによって、一方のネットワークから伝えられた、他方のネットワーク

へ転送された暗号化データの鍵に関する情報（鍵やシード等）を、他方のネットワークへそのまま転送することにより、他方のネットワーク上の装置では該暗号化鍵の再生が可能となるため、コンテンツ受信手段とコンテンツ送信手段との間の暗号復号機能および再暗号化機能が不要となり、中継装置の大幅なコストの低減と、処理速度の高速化を図ることが可能となる。

【００２１】また、好ましくは、他方のネットワーク側の装置と、暗号化されたデータの転送を行っている場合には、他方のネットワーク上の他の装置からの、暗号化が必要なデータの送信要求は拒否するようにしてもよい。このようにすれば、他方のネットワーク側において、異なる暗号化されたデータ転送を未然に防止することが可能となる。

【００２２】好ましくは、前記第１又は第２のいずれか他方のコンテンツ保護手段における前記コンテンツ保護の手続きは、所定の鍵情報を用いて、コンテンツ単位又はサービス単位又はサブユニット単位で行なうようにしてもよい。これによって、他方のネットワーク側の装置との間で、複数の暗号鍵を定義できるようになるため、暗号化されたデータを同時に転送することが可能となり、一方のネットワーク上の装置から複数の暗号化データが転送される場合あるいは一方のネットワーク上に複数の装置がある場合等への対処が可能となる。

【００２３】好ましくは、前記第１及び第２のネットワーク上の装置又はサービス又はサブユニットから、該装置の認証フォーマット（機器証明）の有無を含む構成情報を受信する構成情報受信手段と、前記構成情報受信手段で受信した各構成情報に基づいて、該装置又はサービス又はサブユニットの構成認識を行う構成認識手段とを更に具備するようにしてもよい。これによって、代理構成手段が構成する代理サービスを、自動的に構成することができるようになり、もって、コンテンツ保護手続きに至る手順のプラグアンドプレイでの実現が可能になる。

【００２４】また、好ましくは、前記代理構成手段は、前記第１のネットワークの装置に対してデータを送信する際に、あらかじめ該第１のネットワークの装置に対して自中継装置が代理構成している該データを送信する装置またはサービスまたはサブユニットを通知するようにしてもよい。これによって、この通知を受信した第１のネットワーク上の装置に対して、どこに認証要求を出せばよいかを通知することが可能になる。

【００２５】本発明（請求項１０）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、前記第１のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第１のコンテンツ保護手段と、前記第２のネットワーク上の装置又はサービス又はサブユニットと、自中継装置の間で、コンテンツ保護の手続きを行う第２のコンテンツ保護手段と、前記第１又は第２のいずれか一方のネットワーク上の装置から、自中継装置上の装置又はサービス又はサブユニット宛であり、前記第１又は第２のいずれか一方のコンテンツ保護手段に基づいて暗号化されたコンテンツを受信するコンテンツ受信手段と、前記コンテンツ受信手段で受信したコンテンツを、前記第１又は第２のいずれか他方のコンテンツ保護手段に基づいて暗号化し、前記第１又は第２のいずれか他方のネットワーク上の装置又はサービス又はサブユニット宛に送信するコンテンツ送信手段とを具備し、前記第１のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第１の鍵情報と、前記第２のコンテンツ保護手段における前記コンテンツ保護の手続きで使用する第２の鍵情報とを同一のものとすることを特徴とする。

【００２６】本発明（請求項１１）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置に対して、自通信装置のアドレスを付与した暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは更に自通信装置のアドレスおよび該コンテンツを一意に識別可能な識別子を付与して、送信するコンテンツ送信手段と、前記ネットワーク上の他の装置から、前記仮想チャネル上を介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを受信する受信手段と、この問合せに応答して、前記ネットワーク上の他の装置に対し、該当するサービスまたはサブユニットまたはプラグについての通知をする通知手段とを具備することを特徴とする。

【００２７】本発明（請求項１２）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置から、該ネットワーク上の他の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該ネットワーク上の他の装置が該コンテンツを一意に識別可能な識別子が付与された形で、受信するコンテンツ受信手段と、前記ネットワーク上の他の装置に対して、前記仮想チャネルを介してまたは前記識別子を付与して前記暗号化されたコンテンツを転送しているサービスまたはサブユニットまたはプラグについての問合せを送信する送信手段と、前記ネットワーク上の他の装置から、前記問合せに該当す

るサービスまたはサブユニットまたはプラグについての通知を受信する受信手段とを具備することを特徴とする。

【００２８】本発明によれば、特定の仮想チャネルで転送されている暗号化データの送信、あるいは受信それぞれのサブユニットあるいはプラグを特定することが可能となり、以降の認証・鍵交換で、「このサブユニット（あるいはプラグ）から送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。あるいは、本発明によれば、特定の識別子を持って転送されている暗号化データの送信、あるいは受信それぞれのサブユニットあるいはプラグを特定することが可能となり、以降の認証・鍵交換で、「このサブユニット（あるいはプラグ）から送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００２９】本発明（請求項１３）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置に対して、暗号化されたコンテンツを、送信アドレス、送信ポート、受信アドレスおよび受信ポートの組みで識別されるフローを介して送信または受信するコンテンツ転送手段と、前記ネットワーク上の他の装置との間で、予め定められた論理ポートを用いて、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段とを具備し、前記所定のコンテンツ保護手続きを行なう場合には、これを前記フローの単位で行なうことを特徴とする。

【００３０】好ましくは、前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に前記フローの識別子を付与するようにしてもよい。

【００３１】本発明によれば、フロー毎に異なる鍵の定義ができるようになるため、以降の認証・鍵交換で、「このフローに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００３２】本発明（請求項１５）に係る通信装置は、ネットワークに接続されたインタフェース手段と、前記ネットワーク上の他の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行なうコピープロテクション処理手段と、前記ネットワーク上の他の装置に対して、送信側の装置のアドレスが付与された暗号化されたコンテンツを、ネットワークの仮想チャネル上を介してまたは該送信側の装置が該コンテンツを一意に識別可能な識別子を付与された形で、送信または受信するコンテンツ送受信手段とを具備し、前記所定のコンテンツ保護手続きに含まれる少なくとも一部の手続きにおいてやり取りされる情報に、前記暗号化されたコンテンツのやり取りを行うサービス、サブユニット、仮想チャネルもしくはプラグの識別子、または前記送信側の装置が前記コンテンツを一意に識別可能な識別子のうちの少なくとも一つを付与することを特徴とする。

【００３３】本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグ、あるいは仮想チャネルから送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。あるいは、本発明によれば、認証・鍵交換で、「このサブユニット、あるいはプラグから、あるいは前記特定の識別子を持って、送信、あるいは受信されているデータに関する認証・鍵交換を行いたい」と明示することが可能となり、もって同一ノード同士でも、同時に複数の鍵を定義できるようになるため、複数の暗号化データのやり取りが可能となる。

【００３４】本発明（請求項１６）に係る中継装置は、第１のネットワークに接続された第１のインタフェース手段と、第２のネットワークに接続された第２のインタフェース手段と、第１のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き行う第１のコピープロテクション処理手段と、第２のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続き第２のコピープロテクション処理手段と、前記第１のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第１のインタフェース手段から受信された前記暗号化されたデータを、前記第１のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、前記復号化されたデータを、前記第２のコピープロテクション処理手段で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、前記暗号化されたデータを、前記第２のインタフェース手段へ転送するコンテンツ送信手段とを具備したことを特徴とする。

【００３５】本発明によれば、第１のネットワークを伝送させるデータが保護されるべきコンテンツであり、且つ、第１のネットワークと第２のネットワークの通信帯域が著しく異なる場合のように、第２のネットワークに元のデータとは異なるデータ形式で転送することが求め

られた場合に、変換手段によってデータ形式の変換を行いつつ、第１のネットワーク上の装置から第２のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、両区間（両データ形式）においても、不正コピー等を未然に防ぐことが可能になる。

【００３６】好ましくは、請求項１６に記載の中継装置において、前記第２のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第１のネットワーク側に開示するとともに、前記第１のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第２のネットワーク上の装置またはサービスまたはサブユニット宛に送信するとともに、前記第１のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第２のネットワーク側に開示するとともに、前記第２のネットワーク側の装置から、自中継装置上のものとして開示した装置またはサービスまたはサブユニット宛の情報が受信された場合に、この情報に応じた内容の情報を前記第１のネットワーク上の装置またはサービスまたはサブユニット宛に送信する代理構成手段を更に具備し、前記代理構成手段は、前記第１または第２の一方のネットワーク上の装置と、前記第１または第２の他方のネットワーク上の装置またはサービスまたはサブユニットとの、少なくとも認証手続きおよびまたは鍵交換手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第１または第２の一方のコピープロテクション処理手段を用いて前記一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第１または第２の他方のコピープロテクション処理手段を用いて前記他方のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うようにしてもよい。

【００３７】本発明によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「他方のネットワーク上の装置等」と「一方のネットワーク上の装置」との間において、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がそのコンテンツ保護手続きをそれぞれ終端することで、結局、「他方のネットワーク上の装置等」と中継装置、および中継装置と「一方のネットワーク上の装置」との間で、コンテンツ保護手続きを行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【００３８】また、好ましくは、請求項１６に記載の中継装置において、前記コンテンツ受信手段は、前記第２のコピープロテクション処理手段を用いて、前記第２のネットワーク上の装置またはサービスまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第１のコピープロテクション処理手段を用いて、前記第１のネットワークの装置またはサービスまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うようにしてもよい。なお、前記所定のコンテンツ保護手続きのうち少なくとも一部は、例えば、認証手続きである。このようにすれば、第２のネットワーク上の装置またはサービスまたはサブユニットが信頼に足るデバイスであるかどうかを未然に知ることができるようになり、まず第２のネットワーク上の装置等と認証手続きを行い、その後、第１のネットワーク上の装置等との認証に失敗した場合に、第１のネットワーク上の装置等との認証を改めて行わなくてもよい分、通信資源や処理資源の節約になる。

【００３９】また、本発明に係る通信装置は、第１の装置の制御に供される画面描画のためのプログラムを含む、第１の制御プログラムを受信し、これを稼働するプロセッサ手段と、このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル画面を作成する画面作成手段と、前記パネル画面へのコマンドと、前記第１の装置の制御のためのコマンドとの対応関係を記憶する記憶手段と、前記パネル画面をサブユニットとして第２の装置に公開するサブユニット処理手段と、前記サブユニットへのコマンドを受信した場合、前記記憶手段を参照してこのコマンドを前記第１の装置の制御のためのコマンドに変換して、これを送出する手段とを具備したことを特徴とする。一般に、前記のような制御プログラムを稼働させるためには、仮想マシンと呼ばれ計算環境を用意する必要があるのに対し、パネル画面を通した機器制御は、簡単なコマンド体型を用意するだけでよいため、簡単な計算環境を用意しておけばよい。本発明によれば、前記制御プログラムを持たない第２の装置に対しても、パネル画面という形で、前記第１の装置の制御インタフェースを提供することが可能になる。

【００４０】なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【００４１】また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００４２】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【００４３】（第１の実施形態）図１は、ある家庭のホームネットワークの全体構成の一例である。

【００４４】このホームネットワークには、送信ノード１０１、中継ノード１０２、無線ノード１０３の３つが接続されており、送信ノード１０１と中継ノード１０２は（有線の）ＩＥＥＥ１３９４バス１０４に、中継ノード１０２と無線ノード１０３は無線網にそれぞれ接続されている。ただし、後述するような方法で、各々のノードは互いに通信ができるようになっている。

【００４５】本実施形態では、送信ノード１０１から送出されたＭＰＥＧ映像を、中継ノード１０２で中継し、無線区間を経由して無線ノード１０３に送信する場合を例として説明する。その際に、著作権保護（不正コピーの防止）のために、送信ノード１０１と無線ノード１０３との間で転送されるＭＰＥＧ映像データは暗号化される場合を考える。

【００４６】なお、図１では、３つのノードを示してあるが、もちろん、これらの他にノードが接続されていてもよい（後述する他の実施形態においても同様である）。

【００４７】図２に、送信ノード１０１の内部構造の一例を示す。

【００４８】送信ノード１０１は、内部にＭＰＥＧ映像データを蓄積している装置であり、要求に応じてＭＰＥＧ映像データをＩＥＥＥ１３９４バス１０４を通じて送出する。その際、ＩＥＥＥ１３９４バス上において不法コピーをされることを未然に防止するために、必要な場合には送出するＭＰＥＧ映像データを暗号化して送出する機能を持つ。そのため、ＭＰＥＧ映像データを受信するノードと、認証データ、暗号鍵等の交換を行うための機構も持つ。

【００４９】図２に示されるように、この送信ノード１０１は、ＩＥＥＥ１３９４インタフェース４０１、ＡＶ／Ｃプロトコルの処理を行うＡＶ／Ｃプロトコル処理部４０２、ＡＶ／Ｃプロトコル内のコピープロテクションに関する処理を行うコピープロテクション処理部４０３、ＩＥＥＥ１３９４を通して送受信されるデータのうち、同期チャネルを通してやり取りされるデータについて送受信するＩＳＯ信号送受信部４０４、ＭＰＥＧ映像のストレージであるＭＰＥＧストレージ部４０６、コピープロテクション処理部４０３から暗号鍵Ｋをもらい、ＭＰＥＧ映像を暗号化してＩＳＯ信号送受信部４０４に送出する暗号化部４０５を有する。ここで、コピープロテクション処理部４０３は、認証のためのフォーマットＡｃｅｒｔを持つ。

【００５０】次に、図３に、中継ノード１０２の内部構造の一例を示す。

【００５１】中継ノード１０２は、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ映像データ）を無線区間側にフォワードする機能の他に、ＩＥＥＥ１３９４バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では送信ノード１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能が存在する。

【００５２】図３に示されるように、この中継ノード１０２は、ＩＥＥＥ１３９４インタフェース２０１、無線インタフェース２０２、ＡＶ／Ｃプロトコル処理部２０３、ＩＳＯ信号送受信部２０４、無線区間側の同期チャネルの信号の送受信を行う無線ＩＳＯ信号送受信部２０５、ＩＥＥＥ１３９４バス上のノードの構成情報を収集したり、自らの構成情報（自分がどのような機能を持っているかについての情報等）をＩＥＥＥ１３９４上に広告する機能を持つ１３９４バス構成認識部２０６、ＩＥＥＥ１３９４バス側に対して無線区間側のノードやサービス（サブユニット）を代理で公開したり、無線区間側のノードやサービスへのコマンド等を代理で受け付け、これを無線区間側に必要に応じてプロトコル変換をして送出したり、あるいは無線区間側に対してＩＥＥＥ１３９４側のノード／サービス（サブユニット）の代理公開やコマンドの代理受付／翻訳等を行う代理サブユニット構成部２０７、無線区間上のノードの構成情報を収集したり、自らの構成情報（自分がどのような機能を持っているかについての情報等）を無線区間上に広告する機能を持つ無線区間構成認識部２０９、コピープロテクションに関する処理を行い、１３９４バスと無線区間をまたがるコピープロテクション処理に関しては、やり取りされる情報を透過的にフォワードさせるコピープロテクション制御／フォワード部２１０、無線区間でやり取りされる制御パケットの送受信を行う無線ノード制御パケット送受信部２１１を有する。

【００５３】次に、図４に、無線ノード１０３の内部構造の一例を示す。

【００５４】無線区間においていわゆるＩＥＥＥ１３９４プロトコル（物理レイヤプロトコル、リンクレイヤプロトコル等）が稼働している必要は必ずしもなく、ＩＥＥＥ８０２．１１や無線ＬＡＮ等、任意の無線プロトコルを利用することを想定するが、本実施形態では、特に、いわゆるＱＯＳ機能（同期通信機能）を持つ無線網であることを仮定する。ただし、本実施形態は、無線区間部分にＱＯＳ機能が求められると制限されるものではない。

【００５５】いわゆるＩＥＥＥ１３９４ノードではない無線ノード１０３が、ＩＥＥＥ１３９４バスにつながれたノード（本実施形態では送信ノード１０１）と通信を行うために、前述のように、中継ノード１０２がＩＥＥＥ１３９４バス上のノードや機能（サブユニット）をエ

ミュレートしている。すなわち、無線ノード１０３から見て、中継ノード１０２はいわゆるＩＥＥＥ１３９４バス側のノードや機能の代理サーバとなっている。無線ノード１０３は、これら（ＩＥＥＥ１３９４側のノードや機能）を中継ノード１０２の機能と考え、通信を行うが、実際には中継ノード１０２が必要なプロトコル変換やデータの乗せ換えを行う。

【００５６】図４に示されるように、この無線ノード１０３は、無線インタフェース３０１、無線ノード制御パケット送受信部３０２、コピープロテクション処理部３０３、無線ＩＳＯ信号送受信部３０４、受信した暗号化されたストリーム（ＭＰＥＧ映像等）を、コピープロテクション処理部３０３から渡されるコンテンツキーＫを使ってこれを復号化する暗号復号化部３０５、ＭＰＥＧデコード部３０６、映像を表示するディスプレイ部３０７を有する。

【００５７】無線ノード１０３のコピープロテクション処理部３０３は、後述するように、認証フォーマットＢｃｅｒｔを持ち、その認証の発行機関は、送信ノード１０１（の映像送出サブユニット）の認証フォーマットＡｃｅｒｔの発行機関と同一の発行機関である。

【００５８】次に、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図５／図６（全体のシーケンス例）、図７／図８（送信ノード１０１のフローチャート例）、図９／図１０／図１１（中継ノード１０２のフローチャート例）、図１２／図１３（無線ノード１０３のフローチャート例）を参照しながら説明する。

【００５９】まず、無線ノード１０３は、自分の構成情報を中継ノード１０２に通知する（ステップＳ５０１）。この通知は、無線ノード内にＩＥＥＥ１２１２レジスタを用意し、ここに自分の構成情報を記しておく形で行われてもよい。構成情報とは、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つといったことや、認証・鍵交換のための認証フォーマットを持っていること、などである。ここで、この認証フォーマットが、特定のコピープロテクション機関が定めたフォーマットであることを同時に通知したり、ＩＥＥＥ１３９４向けのコピープロテクションのための認証フォーマットである旨を同時に通知してもよい。

【００６０】ここで、認証について簡単に説明する。

【００６１】ネットワーク上を映画やテレビ番組などの著作権を考慮すべきコンテンツ（データ）を転送する場合、それらのコンテンツは暗号によって保護を行うべきである。なぜなら、これらのデータの転送中に、ネットワーク上で盗聴された場合、不正コピーが可能となってしまうからである。これに対する対策としては、転送するデータの暗号化が有効である。

【００６２】次に問題となるのが、「怪しいものにデータを送っている危険はないか」という問題である。たとえ、データを暗号化して送ったとしても、送った先のノード（暗号を解く鍵を持っている）が悪意を持っている場合（不正コピーをしようと考えている場合）には、やはり解読可能な形でデータを送るべきではない。これに対する対策が認証である。すなわち、この暗号を解く鍵を受信側に渡す前に、受信側が不正を働かないものかどうかの確認をとる（確認が取れた受信側ノードにのみ暗号を解く鍵を渡す）仕組みである。

【００６３】具体的には、予め認証機関が「このノード（あるいはサブユニット）は、不正に働くことはない」と認定したノード（あるいはサブユニット）に対して、「認証フォーマット」と呼ばれるデータを、あらかじめ送信側のノードと受信側のノードとの両方に与えておく。この「認証フォーマット」を正しい形で持っているということは、そのノード（あるいはサブユニット）は信用できる（不正を働かない）と考えることができる。そこで、上記のデータ転送に先立って、送受信ノード（あるいはサブユニット）間で認証フォーマットのやり取りを行い、正しい形で認証フォーマットが確認できた場合に限り、暗号を解くための鍵（もしくは鍵を生成するための元となるデータ）を通知し、その鍵で暗号化されたデータをネットワーク上を転送する、という手法をとる。

【００６４】さて、無線ノード１０３は、このような認証フォーマットをあらかじめ認証機関により与えられており、「暗号化データを正当な形で受信／再生する権利」を持っている。ここで、無線ノード１０３が持っている認証フォーマットを「Ｂｃｅｒｔ」とする。

【００６５】無線ノード１０３は、図５のステップＳ５０１で自分の構成情報を通知する際に、自分は認証フォーマットを有していることを、この構成情報に加えてもよい（ステップＳ８０１）。例えば、図１４のように、構成情報の中に、本無線ノード１０３がＭＰＥＧデコード／ディスプレイ機能を持っており、さらに該機能が認証フォーマットを持っていること、その認証フォーマットがどの発行機関が発行したものか、等の情報を有する。

【００６６】なお、中継ノード１０２が無線ノード１０３の構成を認識する方法としては、この他にも中継ノード１０２が無線ノード１０３に対して構成を問い合わせるパケットを送信し、無線ノード１０３がこれに答える方法等も可能である。

【００６７】さて、この構成情報を受信した中継ノード１０２は、無線ノード１０３が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ７０１）。

【００６８】中継ノード１０２は、無線ノード１０３がＭＰＥＧデコード／ディスプレイ機能を持っていることをＩＥＥＥ１３９４バス側のノードに対して知らせるため、このＭＰＥＧデコード／ディスプレイ機能を、中継

ノード１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ５０２）。具体的には、ＩＥＥＥ１２１２レジスタに「自分はＭＰＥＧデコード／ディスプレイ機能を持っている」旨を記載したり、ＡＶ／Ｃプロトコルでサブユニット構成の問い合わせを受けた場合に、自分がＭＰＥＧデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、ＩＥＥＥ１３９４に接続されたノードは、中継ノード１０２にこの機能が存在すると認識することになる）。

【００６９】そのために、中継ノード１０２は、代理サブユニット構成部２０７内に代理テーブル２０８を持つ。代理テーブル２０８は、図１５／図１６のように、中継ノード１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【００７０】ここでは、図１５のように、無線ノード１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ７０２，Ｓ７０３）。

【００７１】このため、送信ノード１０１から見た中継ノード１０２の構造は図１７のように見えることになる（ステップＳ６０１）。

【００７２】以上は、ＩＥＥＥ１３９４バス側についての説明であったが、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード１０２は、ＩＥＥＥ１３９４バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図１６のような設定がなされ、無線ノードから見た中継ノード１０２の構造は図１８のように見える。

【００７３】さて、中継ノード１０２内にＭＰＥＧデコード／ディスプレイサブユニットがあると認識した送信ノード１０１は、このサブユニットに対して、ＭＰＥＧ映像を転送することを目的に、１３９４バス上に同期チャネル＃ｘを確立し、ＡＶ／Ｃプロトコルにて「この同期チャネル＃ｘ（を受信するプラグ（例えば１３９４ＴＡにて規定されたＡＶ／Ｃにおけるプラグ））と、ＭＰＥＧデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令をだす（ステップＳ５０３，Ｓ６０２）。送信ノード１０１は、このサブユニットが中継ノード１０１にあたるものと解釈しているため、命令の送信先は中継ノード１０２である。

【００７４】これを受信（ステップＳ７０４）した中継ノード１０２は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているＭＰＥＧデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル２０８を参照して、この命令先の実体は無線ノード１０３にあることを認識する（ステップＳ７０５）。

【００７５】よって、ＩＥＥＥ１３９４バスの同期チャネル＃ｘを通して受信したデータを、無線ノード側にフォワードすべく、無線区間の同期チャネル（＃ｙ）の確保を行い（ステップＳ７０６）、さらにＩＳＯ信号送受信部２０４（同期チャネル＃ｘを受信）と無線ＩＳＯ信号送受信部２０５（同期チャネル＃ｙを送信）を接続し、１３９４インタフェース２０１から入力された入力データ（ＩＳＯデータ）を無線区間にフォワードできるようにする（ステップＳ５０４，Ｓ７０７）。

【００７６】さらに、無線ノード１０３に対して、「無線同期チャネル＃ｙを通してデータを送信するので、これを受信し、ＭＰＥＧデコーダに入力し、その結果をディスプレイに表示せよ」との命令を、無線ノード制御パケットの形で送信する（ステップＳ５０５，Ｓ７０８）。

【００７７】図１９に、この無線ノード制御パケットの一例を示す。

【００７８】図１９に示されるように、無線ノード１０３に無線同期チャネル＃ｙを通して送信したデータ（ＭＰＥＧ映像）を、ＭＰＥＧデコード／ディスプレイ機能に転送し、表示することを促す内容となっている。また、この中にこのデータ（ＭＰＥＧ映像）を送信するサブユニット（中継ノード１０２の映像送信機能；実際には、送信ノード１０１の代理でその機能を持っていると広告している）についての情報も併せて通知している。

【００７９】これを受信した無線ノード１０３は、無線同期チャネル＃ｙを通してデータが送られてくることを認識する（ステップＳ８０２）。無線ノード１０３は、このデータの送信元は中継ノード１０２の映像送信サブユニットであると認識する（前述のように、実際のデータ送信元は送信ノード１０１である）。このため、この無線ノード制御パケット内に、「この無線同期チャネルを通して送信されるデータの送信元は中継ノード１０２の映像送信サブユニットである」との情報を含めてもよい。

【００８０】この後、送信ノード１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ６０３，Ｓ５０６）。これを受信した中継ノード１０２は、先に設定したようにこれを無線区間にフォワードする（ステップＳ７０９，Ｓ５０７）。

【００８１】中継ノード１０２は、ステップＳ５０６で暗号化されたＭＰＥＧ映像を受信した時点で、これが暗号化データであることを認識できるが、無線網側に転送する必要があると認識し、これをそのままフォワードする。後に認証・鍵交換の手続きが必要である旨を記憶しておいてもよい。

【００８２】このようにして、暗号化されたＭＰＥＧ映像が無線ノード１０３に到達する（ステップＳ８０３）。このＭＰＥＧ映像には、ソースアドレスとして中継ノード１０２のノードＩＤが含まれていてもよい。このため、無線ノード１０３は、このＭＰＥＧ映像が中継

ノード１０２から到達したものであることまでは認識できるが、この時点で無線ノード１０３はこの暗号を解くための鍵Ｋを有していない（もしくはその鍵を生成するための元となるデータを有していない）ため、この状態で暗号を解いて、ＭＰＥＧ映像を取り出すことはできない。ここで、無線ノード１０３は認証手続きがＭＰＥＧ映像の送信元と必要であることを認識する。

【００８３】そこで、無線ノード１０３（のコピープロテクション処理部３０３）は、認証要求を暗号化データの送信元に対して送信する。先に述べたように、無線ノード１０３には、上記暗号化データの送信元は中継ノード１０２（内の、サブユニット種別＝映像送信サブユニット、かつ、サブユニットＩＤ＝ｂ（ｂ＝０とする）の、サブユニット）であるように認識されている。

【００８４】また、図５のＳ５２１のように、中継ノード１０２に対して、「無線ノードにおいて、無線同期チャネル＃ｙを受信しているのは、サブユニット種別＝ＭＰＥＧデコード／ディスプレイサブユニットで、かつ、サブユニットＩＤ＝ｃ（ｃ＝０とする）の、サブユニットである。無線同期チャネル＃ｙに暗号化データを送信しているのはどのサブユニットか？」という意味合いの問い合わせを送信してもよい。これに対し、中継ノード１０２は、「無線同期チャネル＃ｙに送信しているのは、映像送信サブユニットのサブユニットＩＤ＝０である。」との返答を返す（ステップＳ５２２，Ｓ７３１，Ｓ８３１）。これにより、無線ノード１０３は、認証を行なう先が中継ノードの映像送信サブユニットであることを認識できる。

【００８５】このように、認証要求の宛先を認識し、中継ノード１０２（内の映像送信サブユニットのサブユニットＩＤ＝０）に対し、認証要求を送信する。この送信の仕方として、認証要求パケットの宛先を「中継ノードの映像送信サブユニット（のサブユニットＩＤ＝０）」としてもよいし、認証要求パケットの任意の位置に「映像送信サブユニット（のサブユニットＩＤ＝０）」という情報を入れ、認証要求先は映像送信サブユニット（のサブユニットＩＤ＝０）であると言うことを明確に表示してもよい。前者の場合は、中継ノードの各サブユニット内に認証・鍵交換の手続きが含まれていることを意味する。後者の場合は、中継ノードのある特定の処理部が、一括して、各サブユニットの認証・鍵交換を行なうことを意味する。

【００８６】その際、認証要求には、無線ノード１０３の認証フォーマットＢｃｅｒｔを付与する（ステップＳ８０４，Ｓ５０８）。Ｂｃｅｒｔは、無線ノード１０３のＭＰＥＧデコード／ディスプレイサブユニットの認証フォーマットであってもよい。なお、コピープロテクション処理部は、サブユニット毎（サブユニット種別毎）でなく、サブユニットＩＤ毎に認証フォーマットを用意してもよい。

【００８７】認証要求を受信（ステップＳ７１０）した中継ノードは、代理テーブル２０８を参照して、この認証要求の要求先が実は送信ノード１０１（の映像送信サブユニットのサブユニットＩＤ＝ａ（ａ＝０とする））であることを認識する。

【００８８】中継ノード１０２は、送信ノード１０１に対して、「中継ノードにおいて、同期チャネル＃ｘを受信しているのはＭＰＥＧデコード／ディスプレイサブユニットのサブユニットＩＤ＝０である。同期チャネル＃ｘに暗号化データを送信しているのは、送信ノードのどのサブユニットか？」という意味合いの問い合わせを送信してもよい（ステップＳ５２３，Ｓ６３１，Ｓ７３２）。これに対し、送信ノード１０１は、「同期チャネル＃ｘに送信しているのは、映像送信サブユニットのサブユニットＩＤ＝０である。」との返答を返す（ステップＳ５２４，Ｓ６３１，Ｓ７３２）。

【００８９】このようにして、認証要求の相手を認識したならば、ステップＳ５０８にて受信した認証要求を、中身を変えずに（Ｂｃｅｒｔ等はそのまま残して）送信ノード１０１に対してフォワードする（ステップＳ５０９，Ｓ７１１）。すなわち、宛先アドレスや、認証要求の宛先であるサブユニット以外の認証フォーマット等は、中継ノードは透過的に転送できる。

【００９０】認証要求の転送の際は、先に説明したように、認証要求パケットの宛先を映像送信サブユニット（のサブユニットＩＤ＝０）としてもよいし、認証要求パケットの任意の位置に当該サブユニットを明示する情報を入れ、認証要求先は当該サブユニットであると言うことを明確に表示してもよい。

【００９１】ここで、認証要求の中身を変えずにフォワードすることで、この認証要求はそのままの形で送信ノード１０１に到達することになり、結局、送信ノード１０１と無線ノード１０３との間で、実際の認証手続きは進んでいくことになり、しかも中継ノード１０２をはじめ、その他のノードにはその認証の結果明らかになる鍵の値などの情報を知られることなく、以上の手続きを行っていくことが可能である。

【００９２】認証要求を受け取った送信ノード１０１は、これを中継ノード１０２のＭＰＥＧデコード／ディスプレイサブユニットから送られてきた認証要求であると解釈する（ステップＳ６０４）。その後、Ｂｃｅｒｔから無線ノード１０３のＭＰＥＧデコード／ディスプレイサブユニットを特定できるＩＤ（Ｂｄｉｄ）を抽出し（ステップＳ６０５）、これとともに、やはり同様の認証要求を認証要求の送信元に対して行おうとする。ただし、送信ノード１０１は、Ｂｃｅｒｔが無線ノード１０３の認証フォーマットであるとは意識することはなく、むしろ中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）の認証フォーマットであると意識をしている。

【００９３】この認証要求には、送信ノード１０１（の映像送出サブユニット）の認証フォーマットＡｃｅｒｔと、Ｂｄｉｄとが含まれる。ここで、送信ノード１０１は、該認証要求（ステップＳ５０９）の送信元は中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード１０２となる（ステップＳ６０６，Ｓ５１０）。

【００９４】これを受信（ステップＳ７１２）した中継ノード１０２は、代理テーブル２０８を参照して、この認証手続の本来の要求先が無線ノード１０３（のＭＰＥＧデコード／ディスプレイ機能）であることを認識し、この認証手続要求を、中身を変えずに（Ａｃｅｒｔ等はそのまま残して）無線ノード１０３に対してフォワードする（ステップＳ５１１，Ｓ７１３）。この認証要求の送信元は中継ノード１０２である。

【００９５】これを受け取った無線ノード１０３は、これを中継ノード１０２の映像送信サブユニットから送られてきた認証要求であると解釈する（ステップＳ８０５）。その後、Ａｃｅｒｔから送信ノード１０１の映像サブユニットを特定できるＩＤ（Ａｄｉｄ）を抽出し、認証鍵の交換に必要な残りの手続きを、認証要求の送信元に対して行おうとする。なお、この場合も、無線ノード１０３は、Ａｃｅｒｔが送信ノード１０１の認証フォーマットであるとは意識せず、むしろ中継ノード１０２（の映像送信サブユニット）の認証フォーマットであると意識する。

【００９６】この認証鍵の交換に必要な残りの手続きとして、無線ノード１０３は、認証要求の送信元（と無線ノードが解釈しているノード）に対して認証・鍵交換手続きパケットを送信する（ステップＳ５１２）。この認証・鍵交換手続きパケットには、鍵交換初期値、署名、Ａｃｅｒｔの中に含まれていた送信ノード（の映像送信サブユニット）のデバイスＩＤ（Ａｄｉｄ）等が含まれている（ステップＳ８０６）。ここで、無線ノード１０３は、該認証要求（ステップＳ５１１）の送信元は中継ノード１０２（の映像送信サブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード１０２となる。

【００９７】これを受信した中継ノード１０２は、代理テーブル２０８を参照して、この認証手続きの本来の要求先が送信ノード１０１（の映像送信サブユニット）であることを認識し、この認証手続きパケットを、中身を変えずに送信ノード１０１に対してフォワードする（ステップＳ５１３，Ｓ７１４）。このパケットの送信元は中継ノード１０２である。

【００９８】これと同様の手続きが送信ノード１０１→中継ノード１０２→無線ノード１０３の方向に対しても行われる（ステップＳ５１４，Ｓ５１５，Ｓ６０９，Ｓ７１５，Ｓ８０７）。

【００９９】この認証手続きパケットを受信した送信ノード１０１および無線ノード１０３は、それぞれ、受信したパケットが改ざんされていないかどうかのタンパの確認、相手から送られてきた認証フォーマットが正しいものであるかどうかの確認等を行い、与えられた値を使って共通の認証鍵Ｋａｕｔｈを導き出す。この共通の認証鍵Ｋａｕｔｈは、送信ノード（の映像送信サブユニット）と無線ノード（のＭＰＥＧデコード／ディスプレイ機能）との間で共通に持つ鍵で、この鍵Ｋａｕｔｈを、この両者（送信ノード１０１、無線ノード１０３）以外の他人に知られることなく共有することがこの時点でできるようになる（ステップＳ６０７，ステップＳ６０８，Ｓ８０８）。

【０１００】この認証鍵Ｋａｕｔｈを使って、実際にＭＰＥＧストリームの暗号化を行うコンテンツキーＫの計算ができるようになる。具体的な手順はここでは省略するが、送信ノード１０１から無線ノード１０２に、ＩＥＥＥ１３９４のコピープロテクション方式（５Ｃ方式）のように、交換鍵やシード（種）の値を別途送ることにより、コンテンツキーＫの計算ができるようになっていてもよい（ステップＳ５１８，Ｓ５１９）。

【０１０１】さて、このようにして、送信ノード１０１（の映像送信サブユニット）と無線ノード１０３（のＭＰＥＧデコード／ディスプレイ機能）との間で、コンテンツキーＫの値が共有できるようになった。

【０１０２】ここで、送信ノード１０１が、送信するＭＰＥＧ映像を、コンテンツキーＫを使って、暗号化部４０５にて暗号化し（ステップＳ６１０）、これを１３９４バスの同期チャネル＃ｘを通して中継ノード１０２（のＭＰＥＧデコード／ディスプレイサブユニット）に対して送信する（ステップＳ５１６，Ｓ６１１）。

【０１０３】中継ノード１０２は、送信ノード１０１から同期チャネル＃ｘを通して送られてくる暗号化されたＭＰＥＧ映像を、ＩＳＯ信号送受信部２０４から無線ＩＳＯ信号送受信部２０５を通して、無線同期チャネル＃ｙに送信する（ステップＳ５１７，Ｓ７１６）。

【０１０４】これを受信した無線ノード１０３は、キーＫの値を使ってＭＰＥＧ映像の値を復号化する（ステップＳ８０９，ステップＳ８１０）。復号化されたＭＰＥＧデータは、ＭＰＥＧデコード部３０６にて復号化され（ステップＳ８１１）、これをディスプレイ部３０７にて再生表示する（ステップＳ８１２）。

【０１０５】このように、１３９４バスと無線網との間に代理ノードが存在するような相互接続の環境においても、エンドーエンドのノード同士（本実施形態では送信ノード１０１と無線ノード１０３）が認証手続きや鍵交換手続きを行うことができ、さらにその内容を中継ノード１０２を含め、その他のノードが知ることはできない仕組みとなっている。また、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送も、コピーが不可能

なように経路の全てで暗号化されており、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０１０６】なお、以上の実施形態は、認証手続きや、暗号鍵の交換手続き等を、ノードのサブユニット単位で行ってきたが、無線ノード単位でこれを行うことも可能である。なお、ノード単位で行う例については、次の第２の実施形態で説明するので、例えばこれを適用すればよい。

【０１０７】また、以上の実施形態では、認証および鍵交換のための手続きを暗号化データの受信後に行ってきたが、該手続きは、暗号化データ受信に先だって行ってももちろん構わない。例えば、装置や該当アプリケーションの立ち上げ時に該手続きを行ってもよい。

【０１０８】（第２の実施形態）次に、第２の実施形態について説明する。

【０１０９】第１の実施形態では、送信ノードと無線ノードとが、直接、互いに認証手続きや鍵交換手続きを行ってきた。すなわち、送信ノード（の映像サブユニット）と無線ノード（のＭＰＥＧデコード／ディスプレイ機能）とが、直接、互いを認証し、暗号鍵の交換手続きを行って、暗号化データのやり取りを行ってきた。この際、中継ノードは、送信ノードに対しては無線ノードのＭＰＥＧデコード／ディスプレイ機能の代理機能を果たし、無線ノードに対しては送信ノードの映像送信サブユニットの代理機能を果たしてきたが、上記の認証手続きおよび暗号化データのやり取りの部分については、これらのデータの単なるフォワードを、代理していたサブユニットなり機能なりに行う形であった。

【０１１０】これに対し、第２の実施形態では、中継ノードにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する場合の例を示す。すなわち、送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間で、各々のコピープロテクション手続きは閉じている。つまり、この実施形態においても、中継ノードは、送信ノードあるいは無線ノードに対して代理サービスは提供するものの、コピープロテクションについては、中継ノード自身が認証フォーマットを持ち、中継ノード自身が、１３９４バス区間のＭＰＥＧデータの暗号化転送についての責任を終端するとともに、無線区間のＭＰＥＧデータの暗号化転送についての責任を終端する場合の例である。

【０１１１】図２０に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第１の実施形態と同様である。

【０１１２】図２１に、送信ノード２１０１の内部構造の一例を示す。これも第１の実施形態と基本的には同様である。

【０１１３】次に、図２２に、中継ノード２１０２の内部構造の一例を示す。

【０１１４】中継ノード２１０２は、第１の実施形態と同様に、ＩＥＥＥ１３９４バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では送信ノード２１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能を持つ。

【０１１５】また、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ映像データ）を無線区間側にフォワードする機能を持つが、第１の実施形態と相違する点は、認証データや暗号化等、コピープロテクションに関する手続きがＩＥＥＥ１３９４バス区間と無線区間との両方について、この中継ノード２１０２において終端されており、ＩＥＥＥ１３９４バス側については認証フォーマットＢｃｅｒｔをＩＥＥＥ１３９４コピープロテクション処理部２２０８に、無線区間側については認証フォーマットＣｃｅｒｔを無線区間コピープロテクション処理部２２１２にそれぞれ持ち、１３９４バスの同期チャネルから入力されてきた暗号化データについては、ＩＳＯ信号受信部２２０３にて受信→暗号復号化部２２０４にて暗号復号化→復号化されたＭＰＥＧ映像を、暗号化部２２０５にて再暗号化→無線ＩＳＯ信号送受信部２２０６にて、無線同期信号上に送信、というプロセスを踏む点である。

【０１１６】これらの認証フォーマットは、ＩＥＥＥ１３９４インタフェース毎、あるいは無線区間インタフェース毎に１つずつもっていてもよいし、（代理も含めて）サブユニット毎（サブユニット種別毎）に１つずつ持っていてもよい。

【０１１７】ここで、ＡｃｅｒｔとＢｃｅｒｔは、同じ認証機関（例えばＩＥＥＥ１３９４のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述する無線区間の認証フォーマット（後述するＣｃｅｒｔとＤｃｅｒｔ）については、同じくこの認証機関が発行したものであってもよいし、無線区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【０１１８】次に、図２３に、無線ノード２１０３の内部構造の一例を示す。コピープロテクション処理部２３０３が、無線区間向けの認証フォーマットＤｃｅｒｔを持っていること以外は、基本的には第１の実施形態の無線ノードと同様である。

【０１１９】次に、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図２４／図２５（全体のシーケンス例）、図２６／図２７（送信ノード２１０１のフローチャート例）、図２８／図２９／図３０／図３１（中継ノード２１０２のフローチャート例）、図３２／図３３（無線ノード２１０３のフローチャート例）を参照しながら説明する。

【０１２０】まず、無線ノード２１０３は、自分の構成情報を中継ノード２１０２に通知する（ステップＳ２５０１）。構成情報とは、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つことといったことや、認証のための認証フォーマットを持っていることなどである（図１４参照）。ここで、認証のための認証フォーマットが、無線区間用の認証フォーマットである旨を通知してもよい（ステップＳ２８０１）。

【０１２１】これを受信した中継ノード２１０２は、無線ノード２１０１が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ２７０１）。中継ノード２１０２は、第１の実施形態と同様に、このＭＰＥＧデコード／ディスプレイ機能を、ＩＥＥＥ１２１２レジスタやＡＶ／Ｃプロトコル等を使って、中継ノード２１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ２５０２）。

【０１２２】そのために、中継ノード２１０２は、代理サブユニット構成部２２１０内に代理テーブル２２１４を持つ。この代理テーブル２２１４は、基本的には第１の実施形態と同様であり、図３４／図３５のように、中継ノード２１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【０１２３】ここでは、図３４のように、無線ノード２１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ２７０２，Ｓ２７０３）。

【０１２４】このため、送信ノード２１０１から見た中継ノード２１０２の構造は、図３６のように見えることになる（ステップＳ２６０１）。

【０１２５】以上は、ＩＥＥＥ１３９４バス側についての説明であったが、第１の実施形態と同様に、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード２１０２は、ＩＥＥＥ１３９４バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図３５のような設定がなされ、無線ノードから見た中継ノード２１０２の構造は図３７のように見える。

【０１２６】さて、中継ノード２１０２内にＭＰＥＧデコード／ディスプレイサブユニットがあると認識した送信ノード２１０１は、このサブユニットに対して、ＭＰＥＧ映像を転送することを目的に、１３９４バス上に同期チャンネル＃ｘを確立し、ＡＶ／Ｃプロトコルにて「この同期チャネル＃ｘ（を受信するプラグ）と、ＭＰＥＧデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令を出す（ステップＳ２５０３，Ｓ２６０２）。送信ノード２１０１は、このサブユニットが中継ノード２１０２にあるものと解釈しているため、命令の送信先は中継ノード２１０２である。

【０１２７】これを受信（ステップＳ２７０４）した中継ノード２１０２は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているＭＰＥＧデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル２２１０を参照して、この命令先の実体は無線ノード２１０３にあることを認識する（ステップＳ２７０５）。

【０１２８】ここで、図２０の無線区間は、ＱＯＳ対応の無線ＬＡＮになっており、予め定められた手順を踏めば、パケット廃棄や遅延等の品質劣化無く、転送データを送信先まで転送することが可能であるとする。この無線ＬＡＮ上では、データは図３８のように、イーサネットフレームと同様のフォーマット、すなわち「送信元アドレス、宛先アドレス、データ」のようなフォーマットを持つ、無線フレームで転送される。

【０１２９】さて、ＩＥＥＥ１３９４バスの同期チャネル＃ｘを通して受信したデータを、無線ノード側にフォワードすべく、無線区間のＱＯＳ設定を行う。さらにＩＳＯ信号送受信部２２０３（同期チャネル＃ｘを受信）と無線ＩＳＯ信号送受信部２２０６（ＱＯＳ保証を行なう無線フレームにて送信）を図２２の点線のように接続し（まだ暗号の復号化ができないため）、１３９４インタフェース２２０１から入力されたＩＳＯ入力データを無線区間にそのままフォワードできるようにしてもよい（ステップＳ２５０４，Ｓ２７０６，Ｓ２７０７）。

【０１３０】さらに、無線ノード２１０３に対して、「上記無線フレームを通して、データを送信するので、これを受信し、その結果をディスプレイに表示せよ」との命令を無線ノード制御パケットの形で送信する（ステップＳ２５０５，Ｓ２７０８，Ｓ２８０２）。この制御プロトコルには、ＩＥＥＥ１３９４ＡＶ／Ｃプロトコル、あるいはＩＥＣ６１８８３プロトコルや、これらを変形したものを用いてもよい。後述するように、本実施形態では、無線ＬＡＮ上に同期チャネルの概念はないものの、転送するデータにソースＩＤ（ＳＩＤ）なる領域を設け、無線区間にＱＯＳデータを送信しているノード毎に、転送しているＱＯＳデータを一意に区別できるようになっており、このＳＩＤの値をＩＥＥＥ１３９４の同期チャネルのように、データフローの判別に用いることができる。無線ノード制御パケットの一例を図３９に示す。パケットの送信元は中継ノード２１０２である。

【０１３１】これを受信した無線ノード２１０３は、αなるＳＩＤが付与されて、データがＱＯＳ転送されてくることを認識する。

【０１３２】この後、送信ノード２１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ２５０６，Ｓ２６０３）。コンテンツ鍵はＫ１とする。この暗号鍵は、後述する交換鍵やシードの関数として導出される。

【０１３３】また、この暗号化されたＭＰＥＧ映像を送信するフレームには、同期チャネル番号の他、送信ノー

ドを識別する「送信ノードＩＤ」が含まれていてもよい。

【０１３４】これを受信した中継ノード２１０２は、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信ノードＩＤ」を参照して、このデータを送信しているのが送信ノード２１０１であることを認識し（ステップＳ２７０９）、送信ノード２１０１に対して、「同期チャネル＃ｘを通して、このデータを送出しているのは、送信ノード２１０１のどのサブユニットか」を確かめるため、認証先の問合せを行なう（ステップＳ２５０７，Ｓ２７１０）。この際、データが転送されている同期チャネル番号（＃ｘ）を記載して、送信ノード２１０１が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する自身のサブユニット（本実施形態の場合、中継ノード２１０２のＭＰＥＧデコード／ディスプレイサブユニットのサブユニットＩＤ＝０）も通知する。これは、送信ノード２１０１から見た認証先を通知する役割を持つ。

【０１３５】なお、この認証先問合せパケットと、後述する認証先応答パケットは、認証機関のプライベート鍵でハッシュや暗号化したデータを電子署名として記載しておき、改ざん等が無いことを確認できるようにしてもよい。

【０１３６】さて、認証先問合せを受信（ステップＳ２６０４）した送信ノード２１０１は、同期チャネル＃ｘに対して送信しているデータを受信しているサブユニットが、中継ノード２１０２のＭＰＥＧデコード／ディスプレイサブユニットであることを認識するとともに、自らが該同期チャネル＃ｘに送信しているサブユニットが、映像送信サブユニット（サブユニットＩＤ＝０）であることを、認証先応答パケットとして、中継ノード２１０２に通知する（ステップＳ２５０８，Ｓ２６０５）。

【０１３７】これにより、中継ノード２１０２は、同期チャネル＃ｘにデータを送信しているサブユニットが、送信ノード２１０１の映像送信サブユニット（サブユニットＩＤ＝０）であることを認識できる（ステップＳ２７１１）。

【０１３８】同期チャネル＃ｘにデータを送信しているサブユニットが、送信ノード２１０１の映像送信サブユニットであることを認識した中継ノード２１０２（のＭＰＥＧデコード／ディスプレイサブユニットの代理機能）は、続いて送信ノード２１０１の映像送信サブユニットに対して認証要求を行なう。この認証要求には、中継ノード、あるいは中継ノードのＭＰＥＧデコード／ディスプレイサブユニットの認証フォーマット（Ｂｃｅｒｔ）が共に転送される（ステップＳ２５０９，Ｓ２６０６，Ｓ２６０７，Ｓ２７１２）。この認証要求と認証フォーマットの交換は、第１の実施形態と同様に、送信ノード２１０１（の映像送信サブユニット）から中継ノード２１０２（のＭＰＥＧデコード／ディスプレイサブユニット）に向けても行われる（ステップＳ２５１０，Ｓ２６０８，Ｓ２７１３，Ｓ２７１４）。このように、第２の実施形態においても、認証・鍵交換にサブユニットに関する情報も交換するのは、同じ装置同士の通信でも、通信しているサブユニットが異なれば、異なる鍵の使用ができるようにするためである。

【０１３９】お互いに認証が完了した両ノードは、第１の実施形態と同様に認証・鍵交換手続きを行い（ステップＳ２５１１１，Ｓ２５１１２，Ｓ２６０９，Ｓ２７１５）、認証鍵Ｋａｕｔｈ１を共有する。この認証鍵を使って、送信ノード２１０１は、交換鍵やシードの転送を中継ノード２１０２に対して行ない（ステップＳ２５１２，Ｓ２６１０，，Ｓ２７１６）、結局、中継ノード２１０２では、コンテンツ鍵Ｋ１の値を知ることができるようになる（ステップＳ２７１７）。

【０１４０】以降、転送されてくるコンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像（同期チャネル＃ｘ経由）（ステップＳ２５１３，Ｓ２６１１，Ｓ２６１２）は、中継ノード２１０２にて復号化され（ステップＳ２５１４，Ｓ２７１８）、さらに無線区間用に別に用意されたコンテンツ鍵ｋ２で再暗号化され（ステップＳ２５１５，Ｓ２５１６，Ｓ２７１９）、無線区間上をＱＯＳが保証される形で、無線ノード２１０３に対して送信される（ステップＳ２５１７，Ｓ２７２０，Ｓ２８０３）。この時点では、ＭＰＥＧ映像はＩＳＯ信号送受信部２２０３、暗号復号化部２２０４、暗号化部２２０５、無線ＩＳＯ信号送受信部２２０６というパスを通る。

【０１４１】先に述べたように、このとき中継ノード２１０２が、無線区間側に送信しているデータの区別ができるようにするために、ソースＩＤなる、中継ノード２１０２で一意な値を付与して送出してもよい。ここでは、この一意な値をαとする。すなわち、αの値のついたデータは、ＩＥＥＥ１３９４の同期チャネル＃ｘから受信したデータ（をコンテンツ鍵Ｋ１で復号化し、コンテンツ鍵Ｋ２で再暗号化したもの）である。中継ノード２１０２は、αのＳＩＤを付けて無線区間に送出しているデータは、自身の無線区間側の映像送信サブユニットの代理機能から送信しているデータであることを認識している。

【０１４２】これを受信した無線ノード２１０３の動作は、基本的に先に説明した、暗号化データを受信した中継ノード２１０２の動作と同様である。すなわち、データが暗号化されていることを認識するとともに、例えば受信データに含まれる「送信元アドレス」を参照して、このデータを送信しているのが中継ノード２１０２であることを認識し、中継ノード２１０２に対して、「αなる値を付与して、このデータを送出しているのは、中継ノード２１０２のどのサブユニットか」を確かめるた

め、中継ノードに認証先の問合せを行なう（ステップＳ２５１８，Ｓ２８０４）。

【０１４３】この際、データが転送されているＳＩＤの値（α）を記載して、中継ノード２１０２が、データを送信しているサブユニットを特定できるようにしておくとともに、このデータを受信する受信側のサブユニット（本実施形態の場合、無線ノード２１０３のＭＰＥＧデコード／ディスプレイサブユニットのサブユニットＩＤ＝０）も通知する。これは、中継ノード２１０２から見た認証先を通知する役割を持つ。

【０１４４】認証先問合せを受信（ステップＳ２７２１）した中継ノード２１０２は、ＳＩＤ＝αに対して送信しているデータを受信しているサブユニットが、無線ノード２１０３のＭＰＥＧデコード／ディスプレイサブユニット（サブユニットＩＤ＝０）であることを認識するとともに、自らがＳＩＤ＝αを付与して送信しているサブユニットが、映像送信サブユニットであることを、認証先応答パケットとして、無線ノード２１０３に通知する（ステップＳ２５１９，Ｓ２７２２，Ｓ２８０５）。

【０１４５】これにより、無線ノード２１０３は、ＳＩＤ＝αを付与してデータを送信しているサブユニットが、中継ノード２１０２の映像送信サブユニットであることを認識できる。

【０１４６】ＳＩＤ＝αを付与してデータを送信しているサブユニットが、中継ノード２１０２の映像送信サブユニットであることを認識した無線ノード２１０３（のＭＰＥＧデコード／ディスプレイサブユニット）は、続いて中継ノード２１０２の映像送信サブユニットに対して認証要求を行なう（ステップＳ２５２０，Ｓ２７２３，Ｓ２７２４，Ｓ２８０６）。この認証要求には、無線ノード（または無線ノードのＭＰＥＧデコード／ディスプレイサブユニット）の認証フォーマット（Ｄｃｅｒｔ）が共に転送される。この認証要求と認証フォーマットの交換は、中継ノード２１０２（の映像送信サブユニット）から無線ノード２１０３（のＭＰＥＧデコード／ディスプレイサブユニット）に向けても行われる（ステップＳ２５２１，Ｓ２７２５，Ｓ２８０７）。

【０１４７】お互いに認証が完了した両ノードは、続いて認証・鍵交換手続きを行い（ステップＳ２５２２，Ｓ２５２３，Ｓ２７２６，Ｓ２８０８）、認証鍵Ｋａｕｔｈ２を共有する。この認証鍵を使って、中継ノード２１０２は、交換鍵やシードの転送を無線ノード２１０３に対して行い（ステップＳ２５２４，Ｓ２７２７，Ｓ２８０９）、結局、無線ノード２１０３で、コンテンツ鍵Ｋ２の値を知ることができるようになる（ステップＳ２８１０）。

【０１４８】なお、これまでの説明では送信ノードと中継ノード間の認証・鍵交換と、中継ノードと無線ノード間の認証・鍵交換とは、順次行われる形で説明したが、逆の順番でもよいし、両者を並行して行うことも可能である。

【０１４９】以降、転送されてくるコンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像（ステップＳ２５２５）は、中継ノード２１０２にて復号化され（ステップＳ２５２６）、さらに無線区間用に別に用意されたコンテンツ鍵Ｋ２で再暗号化され（ステップＳ２５２７，Ｓ２５２８，Ｓ２７２８）、無線区間上をＱＯＳが保証される形で、ＳＩＤ＝αが付与された無線フレームの形で無線ノード２１０３に対して送信される（ステップＳ２５２９，Ｓ２７２９）。

【０１５０】今度は、無線ノード２１０３は、先に入手した交換鍵、シードの値を使って、コンテンツ鍵Ｋ２を計算できるので、これを復号化することが可能であり（ステップＳ２５３０，Ｓ２８１１）、これをディスプレイ部２３０７にて再生する（ステップＳ２８１２）。

【０１５１】このように、ＩＥＥＥ１３９４バスと無線網のと間に代理ノードが存在するような相互接続の環境においても、代理機能を提供する中継ノードと送信ノード、および中継ノードと受信ノードが、それぞれの区間で、認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送が可能になる。

【０１５２】もちろん、中継ノード２１０２の「生のＭＰＥＧデータ」が流れる部分、具体的には暗号復号化部２２０４と暗号化部２２０５との間には、データをコピーされる危険が考えられるため、この部分でデータコピーがなされないようにするための工夫（例えば、暗号復号化部と暗号化部を一体のＬＳＩにするなど）がなされていると、この間でプローブをあてるなどしてデータを盗聴（不正コピー）することが実質的に不可能になるため、このような対策を行っておくことが有益である。

【０１５３】（第３の実施形態）次に、第３の実施形態について説明する。

【０１５４】第３の実施形態では、ＩＥＥＥ１３９４上において、ＨＡＶｉ規格（Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｏｆ ｔｈｅ Ｈｏｍｅ Ａｕｄｉｏ／Ｖｉｄｉｏ Ｉｎｔｅｒｏｐｅｒａｂｉｌｉｔｙ（ＨＡＶｉ） Ａｒｃｈｉｔｅｃｔｕｒｅ）等に代表される、ＡＶ／Ｃの上位レイヤに相当するＡＶ機器制御ソフトウェアが稼働している場合における実施形態である。

【０１５５】図４０に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第１の実施形態と同様である。

【０１５６】図４１に、送信ノード４１０１の内部構造の一例を示す。これも第１の実施形態の場合とほぼ同様

であるが、ＩＥＥＥ１２１２レジスタ４４０７を強調のため、追加記述している。ＩＥＥＥ１２１２レジスタ４４０７には、送信ノード４１０１の属性、例えば「どのベンダの製品かを示す情報、例えばＶＴＲやチューナ等といったどのようなジャンルの製品かを示す情報、製造番号、制御ソフトウェアの配置ＵＲＬ、制御アイコン、コマンド一覧」等の情報が含まれる。

【０１５７】次に、図４２に、中継ノード４１０２の内部構造の一例を示す。中継ノード４１０２も、第１の実施形態とほぼ同様の構成であるが、本実施形態のシーケンスを説明する際に必要なＩＥＥＥ１２１２レジスタ４２１３を１３９４バス構成認識部４２０６内に特に記した点と、ＨＡＶｉ処理部４２１２を持つ点が第１の実施形態と異なる。ＨＡＶｉ処理部４２１２には、いわゆるＨＡＶｉバイトコードの処理を行う仮想マシン（ＶＭ）が存在する。また、本実施形態においては、制御画面の記述を行う「パネルサブユニット」の代理機能を代理サブユニット構成部４２０７が持つ。

【０１５８】次に、図４３に、無線ノード４１０３の内部構造の一例を示す。これについても、第１の実施形態の場合と基本的には同様である。

【０１５９】次に、ＨＡＶｉ環境における、実際のコピープロテクションを施した上でのＭＰＥＧ映像全体のシーケンスについて、図４４／図４５（全体のシーケンス例）、図４６／図４７（送信ノード４１０１のフローチャート例）、図４８／図４９／図５０（中継ノード４１０２のフローチャート例）、図５１／図５２（無線ノード４１０３のフローチャート例）を参照しながら説明する。

【０１６０】まず、無線ノード４１０３は、自分の構成情報を中継ノード４１０２に通知する（ステップＳ４５０１）。このとき、これらの構成情報は、ＩＥＥＥ１２１２レジスタ形式の情報として中継ノード４１０１に送付するものとする。すなわち、中継ノード４１０２が、無線ノード４１０３に対して「ＩＥＥＥ１２１２で規定されるＣＳＲ（コマンド・ステータスレジスタ）空間の、このアドレスに相当する部分についての情報」を要求し、これに無線ノード４１０３が答える形でこのやり取りが行われてもよい。ここで、前述のように、この構成情報には、自分（無線ノード）がＭＰＥＧデコード／ディスプレイ機能を持つといったことや、認証のための認証フォーマットを持っていること、等が含まれる。ここで、無線ノード４１０３が持っている認証フォーマットをＢｃｅｒｔとする。

【０１６１】これを受信した中継ノード４１０２は、無線ノード４１０１が認証フォーマットを持つことや、ＭＰＥＧデコード／ディスプレイ機能を持っていることを確認する（ステップＳ４７０１）。中継ノード４１０２は、無線ノード４１０１がＭＰＥＧデコード／ディスプレイ機能を持っていることをＩＥＥＥ１３９４バス側のノードに対して知らせるため、このＭＰＥＧデコード／ディスプレイ機能を、中継ノード４１０２自身のサブユニットとしてＩＥＥＥ１３９４バス側に広告する（ステップＳ４５０２）。具体的には、自身のＩＥＥＥ１２１２レジスタに「自分はＭＰＥＧデコード／ディスプレイ機能を持っている」旨を記載したり、ＡＶ／Ｃプロトコルでサブユニット機能の問い合わせを受けた場合に、自分がＭＰＥＧデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、送信ノード４１０１等のＩＥＥＥ１３９４に接続されたノードは、中継ノードにこの機能が存在すると認識することになる）。

【０１６２】そのために、中継ノード４１０２は、代理テーブル４２０８を持つ。代理テーブル４２０８は、図５３／図５４のように、中継ノード４１０２が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【０１６３】ここでは、図５３のように、無線ノード４１０３のＭＰＥＧデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップＳ４７０２，Ｓ４７０３）。

【０１６４】以上と逆の手続きがＩＥＥＥ１３９４バス４１０４上の送信ノード４１０１の代理登録を無線区間側に対してみせる形で行われる（ステップＳ４５０３，Ｓ４５０４）。すなわち、送信ノード４１０１のＩＥＥＥ１２１２レジスタ４４０７に、自分が映像送信機能を持つこと、およびパネル機能（制御画面機能）を持つことを記述しておき、これを中継ノード４１０２が読み込む（ステップＳ４６０１，Ｓ４７０４）。この送信ノード４１０１の機能を、中継ノード４１０２の機能として、代理して無線区間側のＩＥＥＥ１２１２相当機能（無線区間側のＣＳＲ空間）に反映し、無線ノード４１０３側には、上記映像送信機能、およびパネル機能が中継ノード４１０２の機能であるものとして認識してもらう。この対応関係を、代理テーブル４２０８に図５４のように反映する（ステップＳ４７０５）。

【０１６５】このようにして代理テーブル４２０８は、図５３／図５４のように構成される。また、送信ノード４１０１から見た中継ノード４１０２の内部構造を図５５に、無線ノード４１０３から見た中継ノード４１０２の内部構造を図５６に、それぞれ示す。

【０１６６】なお、この時点で、ステップＳ４５０３の送信ノード構成情報の中に、送信ノード４１０１を制御するためのＨＡＶｉのバイトコードが含まれており、中継ノード４１０２は送信ノード４１０１の代理サーバ、すなわちＤＣＭ（デバイスコントロールモジュール）の機能を有していてもよい。この場合、このバイトコードは、中継ノード４１０２のＨＡＶｉ処理部４２１２内の仮想マシン上で稼働することになる。

【０１６７】さて、中継ノード４１０２にパネル機能が

あるものと認識した無線ノード４１０３は、中継ノード４１０２の（バネルサブユニット）に対して、バネルの表示要求のコマンドを送出する（ステップＳ４５０５，Ｓ４８０２）。これを受信（ステップＳ４７０６）した中継ノード４１０２は、代理テーブル４２０８を参照し、このバネル機能の実体が送信ノード４１０１に存在していることを認識し、前記バネル表示要求コマンドを送信ノード４１０１に対してフォワードする（ステップＳ４５０６，Ｓ４７０７）。

【０１６８】これを受信（ステップＳ４６０１）した送信ノード４１０１は、ＡＶ／Ｃプロトコルにてバネル応答（つまり、制御画面の送信）を行う。送信先は、中継ノード４１０２である（ステップＳ４６０３，Ｓ４５０７）。これを受信（ステップＳ４７０８）した中継ノード４１０２は、代理テーブル４２０８を参照して、これを無線ノード４１０３にフォワードする（ステップＳ４７０９，Ｓ４５０８，Ｓ４８０３）。

【０１６９】ここで、図５７に、無線ノード４１０３に送られてきた制御画面の一例を示す。この制御画面（バネル）では、６つの映画のタイトルを表示したボタンが提供される。これらのボタンは、例えば「ボタン１」、「ボタン２」、…等の名前が付けられており、ユーザがあるボタンを押すと、例えば「ボタン１が押されました」というコマンドの形で、バネルの送信元に送られる仕組みとなっているものとする。

【０１７０】さて、無線ノード４１０３は、中継ノード４１０２が提供していると認識している映像送信サービスを受けようと考え（実際に提供しているのは送信ノード４１０１）、無線ノード制御パケットを使って（ステップＳ４５０９）、映像を流すための無線同期チャネル＃ｙを確保し、このチャネルを中継ノード４１０２の映像送信サブユニットに接続するためのコマンドを中継ノード４１０２に対して発行する（ステップＳ４８０４）。これを受信した中継ノード４１０２は、代理テーブル４２０８を参照して、実際にこのＡＶ／Ｃコマンドが発行されるべきノード（送信ノード４１９１）を確認し、ＩＥＥＥ１３９４バス上に必要な帯域を確保するとともに（同期チャネル＃ｘ）、内部のＩＳＯ信号送受信部４２０４を設定して、ＩＥＥＥ１３９４バスの同期チャネル＃ｘと無線同期チャネル＃ｙとを相互に接続する（ステップＳ４７１０，Ｓ４７１１，Ｓ４７１２，Ｓ４５１０）。また、中継ノード４１０２は、送信ノード４１０１に対し、同期チャネル＃ｘを映像送信サブユニットに接続するコマンドを発行する（ステップＳ４５１１，Ｓ４７１３）。これを受信（ステップＳ４６０４）した送信ノード４１０１は、映像送信サブユニットの実体である内部の映像ストリームの流れるバス（図４１で２重矢印になっている部分）をＩＥＥＥ１３９４バスの同期チャネル＃ｘに接続する。

【０１７１】これと前後して、無線ノード４１０３のユーザは、見たい映像を選択するために図５７のバネルの中から適当な番組を選択すべく、制御画面のボタンを押す（例えば、マウスを使ってクリックする、ペン入力する、タッチする、など）。この操作は、中継ノード４１０２に伝達され、これは代理テーブル４２０８の参照を経て送信ノード４１０１へのコマンドに変換される（ステップＳ４８０５，Ｓ４７１４，Ｓ４７１５，Ｓ４６０５，Ｓ４５１２，Ｓ４５１３）。

【０１７２】この後、送信ノード４１０１は、同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像を転送する（ステップＳ４５１４，Ｓ４６０６）。これは、中継ノード４１０２にて中継され、無線ノード４１０３に到達する（ステップＳ４７１６）。

【０１７３】後の手続きは、第１の実施形態の場合と同様であり、暗号化されたＭＰＥＧ映像が無線ノード４１０３に到達する（ステップＳ４８０６）が、この時点で無線ノード４１０３はこの暗号を解くための鍵を有していないため、ＭＰＥＧ映像の送信元と認証手続きを開始する。認証手続き以降の手続きについては第１の実施形態と同様であるので、ここでの詳細な説明は省略する。

【０１７４】なお、第１の実施形態に従えば、認証は送信ノード４１０１の映像送信サブユニットに相当する機能と、無線ノードの映像受信サブユニットに相当する機能ととの間で行われると考えられるが、第３の実施形態の場合には、このような認証方式の他に、送信ノード４１０１のバネルサブユニットが認証の対象となるような方式も考えられる。この場合は、送信ノード４１０１のバネルにデバイスＩＤが割り当てられることになる。

【０１７５】なお、ＨＡＶｉにおいては、送信ノード４１０１から送られてくるバイトコードであるＤＣＭ等の中に、送信ノード４１０１を制御するための制御画面情報が含まれる場合がある。このようなモジュールをＤＤＩ（データドリブンインタラクション）と呼ぶ。このようなモジュールは、例えば中継ノード４１０２内のＨＡＶｉ処理部４２１２にて展開され、制御画面が生成される。本実施形態では、この制御画面（あるいは、それと同等の機能を持つ制御画面）を無線ノード側に見せることを考える必要があるが、この場合は、代理サブユニット構成部４２０７が、このＤＤＩに含まれる画面構成情報を認識して（例えば、画面構成のためのシステムコールをイベントして認知して、生成される最終画面の概要を推察する方法や、完成した制御画面をもとにする方法等が考えられる）、バネルとしてこの制御画面を再構成し、無線区間に「バネルサブユニット」としてこれを公開する方法が考えられる。この場合には、代理テーブル４２０８には、このバネルと、ＤＤＩで生成されるべきＨＡＶｉやＡＶ／Ｃのコマンド（中継ノード４１０２から送信ノード４１０１に対して発行される）の対応テーブルが用意されることになる。この方法は、無線ノード４１０３内にＨＡＶｉバイトコードの仮想マシンが存在

しなくても有効であるため、ＨＡＶｉ仮想マシンを持たない無線ノード４１０３から、ＨＡＶｉ機器の制御を可能とする方法である。

【０１７６】（第４の実施形態）次に、第４の実施形態について説明する。

【０１７７】図５８に、本実施形態の全体構成の一例を示す。

【０１７８】図５８に示されるように、第４の実施形態では、ある家庭のホームネットワークであるＩＥＥＥ１３９４バス６１０４と、公衆網（ここでは、一例としてインターネットとするが、電話網等でもよい）６１０５とが、ホームゲートウェイ６１０２で接続され、送信ノード６１０１と受信ノード６１０３との間で、認証手続き、暗号化の手続きを経た上で例えば映像データのやり取りを行う。ここで、インターネット６１０５（のアクセス網部分）は、ＩＥＥＥ１３９４バス６１０４と比べて通信帯域が非常に細く、ＩＥＥＥ１３９４バスでやり取りされる映像情報（一例としてＭＰＥＧ２映像であるとする）は、帯域が足りずに通せないため、ホームゲートウェイ６１０２においてトランスコーディング、つまりＭＰＥＧ２符号からＭＰＥＧ４符号への符号変換を行った上で、伝送を行うことを考える。

【０１７９】第４の実施形態においても、第２の実施形態と同様に、ホームゲートウェイにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する。すなわち、送信ノードとホームゲートウェイ、ホームゲートウェイト受信ノードとで、おのおのコピープロテクション手続きは閉じている。この実施形態においても、ホームゲートウェイは、送信ノードや受信ノードに対して代理サービスを提供し、また、コピープロテクションについては、ホームゲートウェイ自身が認証フォーマットを持ち、ホームゲートウェイ自身が１３９４バス区間および無線区間のＭＰＥＧデータの暗号化転送についてのそれぞれの責任を終端する。

【０１８０】次に、図５９に、送信ノード６１０１の内部構造の一例を示す。これは基本的にはこれまでの実施形態と同様の構成である。

【０１８１】次に、図６０に、ホームゲートウェイ６１０２の内部構造の一例を示す。

【０１８２】ホームゲートウェイ６１０２の基本的な構成は、無線インタフェースではなくインターネットインタフェース６２０２を有している点、代理サブユニット構成部ではなく代理ホームページ作成部６２１０を有している点、ホームページの作成・蓄積部６２１１を有している点、暗号復号化部６２０４と暗号化部６２０５との間にＭＰＥＧ２／ＭＰＥＧ４変換部６２１４を有している点を除くと、第２の実施形態の中継ノードの構成とほぼ同様である。上記の相違点については順次説明していく。

【０１８３】ホームゲートウェイ６１０２は、インターネット側のノードに対してＩＥＥＥ１３９４バス側のノード（本実施形態では、送信ノード２１０１）の代理サーバとなり、ＩＥＥＥ１３９４バス側のノードの機能を代理で提供する機能を持つ。送信ノード６１０１が提供しているサービス（本実施形態の場合、映像送信サービス）には、ホームゲートウェイ６１０２が提供しているホームページを介してアクセスすることが可能である。ここで、受信ノード６１０３からは、送信ノード６１０１のサービスは、ホームゲートウェイ６１０２のホームページを介して見えるため、これをホームゲートウェイ６１０２が提供するＩＰ（インターネット）上のサービスとして解釈されてもよい。

【０１８４】また、ホームゲートウェイ６１０２は、第２の実施形態と同様に、ＩＥＥＥ１３９４バス側から受信したデータ（ＭＰＥＧ２映像データ）をインターネット側にフォワードする機能を持つが、認証やデータの暗号化等、コピープロテクションに関する手続きがＩＥＥＥ１３９４バス区間とインターネット区間との両方について、このホームゲートウェイ６１０２において終端されている。ＩＥＥＥ１３９４バス側については、認証フォーマットＢｃｅｒｔをＩＥＥＥ１３９４コピープロテクション処理部６２０８に、インターネット区間側については、認証フォーマットＣｃｅｒｔをインターネット側コピープロテクション処理部６２１２にそれぞれ持ち、ＩＥＥＥ１３９４バスの同期チャネルから入力されてきた暗号化データについては、ＩＳＯ信号送受信部６２０３にて受信→暗号復号化部２２０４にて暗号復号化→復号化されたＭＰＥＧ２映像をＭＰＥＧ２／ＭＰＥＧ４変換部６２１４にてトランスコード→ＭＰＥＧ４映像を暗号化部６２０５にて再暗号化→ＡＶ信号送受信部６２０６にてインターネット側に送信、というプロセスを踏む。

【０１８５】ここで、ＡｃｅｒｔとＢｃｅｒｔは、同じ認証機関（例えばＩＥＥＥ１３９４のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述するインターネット区間の認証フォーマット（後述するＣｃｅｒｔとＤｃｅｒｔ）については、同じくこの認証機関が発行したものであってもよいし、インターネット区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【０１８６】なお、本実施形態においては、認証フォーマット（Ａｃｅｒｔ～Ｄｃｅｒｔ）は、ノード（あるいはネットワークインタフェース）毎に１つ持つのではなく、サブユニット毎（サブユニット種別毎）、あるいはインターネットアプリケーション毎に１つ持ってもよい。すなわち、異なるインターネットアプリケーションでは、異なる認証フォーマットを用いてもよい。ここで、フローとは、インターネットの（送信アドレス、送信ポート、受信アドレス、受信ポート）の組で表現され

る一連のデータ流を指す。

【０１８７】次に、図６１に、受信ノード６１０３の内部構造の一例を示す。

【０１８８】コピープロテクション処理部６３０３がインターネット向けの認証フォーマットＤｃｅｒｔを持っている。第２の実施形態との相違点は、インタフェース（インターネットインタフェース６３０１、制御パケット送受信部６３０２、ＡＶ信号送受信部６３０４）がインターネット対応となっている点である。ここで、制御パケット送受信部６３０２はＴＣＰ、ＡＶ信号送受信部６３９４はＵＤＰのトランスポートプロトコルを持つパケットの送受信モジュールであってもよい。

【０１８９】次に、実際のコピープロテクションを施した上での映像送信全体のシーケンスについて、図６２／図６３（全体のシーケンス例）、図６４／図６５（送信ノード６１０３のフローチャート例）、図６６／図６７／図６８／図６９（ホームゲートウェイ６１０２のフローチャート例）、図７０／図７１（受信ノード６１０３のフローチャート例）を参照しながら説明する。

【０１９０】まず、ホームゲートウェイ６１０２は、送信ノード６１０１のＩＥＥＥ１２１２レジスタの読み込みなどを通して、送信ノードについての属性や構成情報を収集する（ステップＳ６５０１，Ｓ６６０１，Ｓ６７０１，Ｓ６５０２，Ｓ６６０２，Ｓ６７０２）。これを通して、ホームゲートウェイ６１０２は、送信ノード６１０１が映像送信機能を持つこと、パネル機能を持つこと、認証フォーマットを持っていること等を把握する。

【０１９１】これを受けて、ホームゲートウェイ６１０２は、送信ノード６１０１を遠隔制御するためのホームページを作成する（ステップＳ６５０３）。基本的には、送信ノード６１０１が持つパネルと同様の画面を「送信ノード制御用ホームページ」として作成する。ホームページ上に配置された制御用のボタン等は、それぞれ送信ノード６１０１のパネルサブユニットのボタンに対応する等して、代理ホームページ作成部６２１０内の変換テーブルに対応の一覧が記述される。例えば、送信ノード６１０１のパネルサブユニットに「再生」とかかれているボタンが存在する場合には、該ホームページにも「再生」とかかれているボタンを用意して、この関係を前記変換テーブルに記述しておく。もし、このホームページのユーザがこのボタンを押した場合には、ホームゲートウェイ６１０２から送信ノード６１０１のパネルサブユニットの「再生」ボタンに対して「ボタンが押された」というインタラクションが返る形となる。図７２（ａ）に送信ノード６１０１のパネルサブユニットの持つパネルの一例を、図７２（ｂ）にホームゲートウェイ６１０２の作成した送信ノード制御用ホームページの一例をそれぞれ示す。

【０１９２】さて、インターネット上の受信ノード６１０３は、インターネットを介してこのホームゲートウェイ６２０１にアクセスし、送信ノード６１０１の制御画面を含むホームページを要求し、このホームページが送付される（ステップＳ６５０４，Ｓ６８０１，Ｓ６７０３）。これを見て、受信ノード６１０３のユーザは、画面上の映像送信を要求するボタン（例えば、図７２（ｂ）の「再生」ボタン）を押したものとする。この結果、例えば「再生ボタンが押された」、というインタラクションが、インターネット経由でホームゲートウェイにＨＴＴＰを通じて通知される（ステップＳ６５０５，Ｓ６８０２，Ｓ６７０４）。

【０１９３】この通知と前後して、ホームゲートウエイ６１０２と受信ノード６１０３との間で、やり取りされるストリームが転送されるＩＰフロー、すなわち（送信ＩＰアドレス、送信ポート、受信ＩＰアドレス、受信ポート）の組の決定や、セッション制御（符号化方式や認証方式等）のネゴシエーション等が行なわれる（ステップＳ６５０５，Ｓ６７０５，Ｓ６８０３）。例えば、ＲＴＳＰ（リアルタイムトランスポートストリーミングプロトコル）やＳＤＰ（セッションデスクリプションプロトコル）等を用いて、符号化方式や認証の方式、ポートの番号の決定などが行われる。

【０１９４】ホームゲートウエイ６１０２は、これらの処理を受け、映像送信を行なう実体は、送信ノード６１０１の映像送信サブユニットであることを認識し、送信ノード６１０１に対してＡＶ／Ｃプロトコル等で、データ転送のための同期チャネル＃ｘの設定や、映像送信サブユニットに対して、映像送信の要求などのコマンドを発行する（ステップＳ６５０６）。

【０１９５】これを受けて、送信ノード６１０１から同期チャネル＃ｘを通して、暗号化されたＭＰＥＧ映像がホームゲートウエイ６１０２に対して送出される（ステップＳ６５０７，Ｓ６６０３，Ｓ６６０４）。その後は、第２の実施形態のＩＥＥＥ１３９４側の手順と同様の手順で、認証先問合せ／応答、認証要求、認証・鍵交換手続き、交換鍵／シード転送等が行われ、ホームゲートウエイ６１０２にてコンテンツ鍵Ｋ１の計算ができるようになる（ステップＳ６５０８～Ｓ６５１４，Ｓ６６０５～Ｓ６６１１，Ｓ６７０６～Ｓ６７１５）。

【０１９６】以降、同期チャネル＃ｘを通して暗号化されたＭＰＥＧ映像（ステップＳ６５１５，Ｓ６６１２，Ｓ６６１３）を受信したホームゲートウエイ６１０２は、暗号復号化部６２０４にて、これをコンテンツ鍵Ｋ１を用いてＭＰＥＧ２映像に復号化する（ステップＳ６５１６，Ｓ６５１７，Ｓ６７１６）。次に、抽出したＭＰＥＧ２映像を、ＭＰＥＧ２／ＭＰＥＧ４変換部６２１４でＭＰＥＧ４映像にトランスコードする（ステップＳ６５１８）。このＭＰＥＧ４映像を、コンテンツ鍵Ｋ２を用いて、暗号化部６２０５で再暗号化し（ステップＳ６５１９，Ｓ６５２０，Ｓ６７１７，Ｓ６７１８）、これをＩＰパケット化する。その場合、先のセッション制

御の手順で決めたように、送信ＩＰアドレスはＣ（ホームゲートウエイのＩＰアドレス）、送信ポート番号はｃ、受信ＩＰアドレスはＤ（受信ノードのＩＰアドレス）、受信ポート番号はｄであるようなＩＰパケットを生成する（ステップＳ６５２１，Ｓ６７１９）。

【０１９７】これを受信した受信ノード６１０３は、受信したデータが暗号化されていることを認識する（ステップＳ６８０４）。受信ノード６１０３は、このデータを送信しているのは、到着したパケットのＩＰヘッダを参照すること等により、ホームゲートウエイ６１０２であることを認識し、ホームゲートウエイ６１０２に対して、認証要求を送信する（ステップＳ６５２２，Ｓ６８０５）。この認証要求のパケットもＩＰパケットでもよい。認証要求のためのポート番号は、認証を行なう手続きに予め割当てられている番号を用いてもよい。この際、この認証要求のパケットに、ストリーム転送のフローＩＤ（Ｃ、ｃ、Ｄ、ｄ）を付与して転送する。このことにより、ホームゲートウエイ６１０２は、どのフローに対する認証要求であるかを認識することができる。図示はしていないが、この認証要求には、受信ノードの（本ストリーム用の）認証フォーマット等も含まれている。

【０１９８】また、トランスポートプロトコルとしてＲＴＰ（Ｒｅａｌｔｉｍｅ　Ｔｒａｎｓｐｏｒｔ　Ｐｒｏｔｏｃｏｌ）を用いていること等を同時に伝えてもよい。

【０１９９】これを受けてホームゲートウエイ６１０２は、フロー（Ｃ、ｃ、Ｄ、ｄ）のための認証要求であることを認識し、このフローのための認証フォーマットを含んだ認証要求を、受信ノード宛てに送り返す（ステップＳ６５２３，Ｓ６７２０～Ｓ６７２２，Ｓ６８０６，Ｓ６８０７）。このとき、この認証要求には前記フローＩＤ等が含まれる。

【０２００】次に、両者は、認証・鍵交換手続き、交換鍵／シードの転送等を、ＩＰパケット上で行う（ステップＳ６５２４～Ｓ６５２６，Ｓ６７２３，Ｓ６７２４，Ｓ６８０８～Ｓ６８１０）。これにより、受信ノード６１０３は、コンテンツ鍵Ｋ２の生成が行なえるようになっている。

【０２０１】よって、以降、コンテンツ鍵Ｋ２にて暗号化された、フロー（Ｃ、ｃ、Ｄ、ｄ）を通して送られてくるＭＰＥＧ４データ（ステップＳ６５２７～Ｓ６５３３，Ｓ６７２５，Ｓ６７２６，Ｓ６８１１）は、上記のように用意されたコンテンツ鍵ｋ２にて復号化することが可能となる（ステップＳ６５３４）。復号化されたＭＰＥＧ４データは、ＭＰＥＧデコード部６３０６にて復号化され（ステップＳ６８１２）、これをディスプレイ部６３０７にて再生する（ステップＳ６８１３）。

【０２０２】このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイと送信ノード、およびホームゲートウェイと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２０３】第２の実施形態と同様に、ホームゲートウェイ６１０２において、「生のＭＰＥＧデータ」が流れる部分、具体的には暗号復号化部６２０４、ＭＰＥＧ２／ＭＰＥＧ４変換部６２１４、暗号化部６２０５との間は、データコピーがなされないようにするための工夫、例えば一体のＬＳＩに封止する等の対策を立てておいてもよい。

【０２０４】（第５の実施形態）次に、第５の実施形態について説明する。

【０２０５】第４の実施形態が、公衆網（インターネット）を介して家庭網にアクセスし、コピープロテクションを考慮した上で家庭網上の端末とインターネット上の端末間でコンテンツをやり取りする場合であったのに対し、第５の実施形態は、公衆網を介して家庭網間でコンテンツをやり取りする場合である。

【０２０６】図７３に、本実施形態の全体構成図を示す。

【０２０７】図７３に示されるように、第５の実施形態では、２つの家庭網８１０５，８１０７が公衆網（ここでは、一例としてインターネットとするが、Ｂ－ＩＳＤＮ等でもよい）８１０６にて接続されている。第１の家庭網８１０５上の送信ノード８１０１から、コピープロテクションを考慮した形で、ＡＶコンテンツを第２の家庭網８１０７上の受信ノード８１０４に送信する。ここで、第４の実施形態では、公衆網部分の通信帯域が非常に細い場合の例を示したが、本実施形態では、公衆網の通信帯域は十分な容量を持つものとする。

【０２０８】第５の実施形態においては、第１の実施形態の中継ノードと同様に、ホームゲートウェイ８１０２，８１０３にて、ＩＥＥＥ１３９４バス８１０５，８１０７上のサービスを公衆網側に代理サービスする。すなわち、インターネット上からは、インターネットのサービスとして、家庭網上の装置やサービス、コンテンツが見える。また、ホームゲートウェイ８１０２，８１０３は、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りについてはこれらをフォワードする。

【０２０９】送信ノード８１０１や受信ノード８１０４は、基本的には第４の実施形態と同様の構成である。

【０２１０】図７４に、ホームゲートウェイ８１０２，８１０３の内部構造の一例を示す。

【０２１１】ホームゲートウェイ８１０２の基本的な構

成は、コピープロテクションを終端しない点（これは、第１の実施形態の中継ノードと同様）、および暗号の符号化・復号化・符号変換を行わない点（これも、第１の実施形態の中継ノードと同様）を除き、第４の実施形態のホームゲートウェイの構成とほぼ同様である。

【０２１２】図７５に、全体のシーケンスの一例を示す。

【０２１３】ここでは、第２の家庭網８１０７のユーザが、ホームゲートウェイ８１０３の制御画面を使って、送信ノード８１０１のコンテンツを、インターネット８１０６を介して受信ノード８１０４に配信させる場合を考える。

【０２１４】まず、第４の実施形態と同様に、ステップＳ８３０１の構成認識と、ステップＳ８３０２の送信ノード制御用ホームページ作成が行われる。

【０２１５】第２の家庭網８１０７のユーザは、ホームゲートウェイ８１０３を操作し、ホームゲートウェイ８１０２から送信ノード制御用のホームページ（制御画面）を持ってくる（ステップＳ８３０３）。また、例えば図７６に例示するような受信ノード８１０４の制御画面も同時に開く。そこで、図７６のように、送信ノード内のコンテンツ一覧から、適当なものを例えばドラッグアンドドロップするなどして、ホームゲートウェイ８１０３に映像配信を命令する（ステップＳ８３０４）。

【０２１６】すると、第４の実施形態と同様に、映像送信要求がホームゲートウェイ８１０２に（インターネットコマンドとして）発行され（ステップＳ８３０５）、これがホームゲートウェイ８１０２にてＡＶ／Ｃプロトコルコマンドに翻訳され、送信ノード８１０１から受信ノード８１０４間の通信パス（ＩＥＥＥ１３９４バス８１０５上の同期チャネル＃ｘ、インターネット上のコネクション、ＩＥＥＥ１３９４バス上の同期チャネル＃ｙ）が設定される（ステップＳ８３０６，Ｓ８３０７）。この上を、暗号鍵Ｋで暗号化されたＭＰＥＧ２映像が配信される（ステップＳ８３０８～Ｓ８３１０）。

【０２１７】第１の実施形態と同様に、これを受信した受信ノード８１０６は、送信元に認証要求を発行する（ステップＳ８３１１）。受信ノード８１０４は、この映像はホームゲートウェイ８１０３から配信されていると解釈しているため、この認証要求はホームゲートウェイ８１０３に対して行われる。

【０２１８】ホームゲートウェイ８１０３は、第４の実施形態と同様に、内部の変換テーブル８２１１を参照して、これをホームゲートウェイ８１０２にフォワードする。これは、ホームゲートウェイ８１０３は、映像の配信元がホームゲートウェイ８１０２であると解釈しているからである。このフォワードは、認証要求８３１１の中身を変えない形で、インターネットバケットで行われる（ステップＳ８３１２）。同様に、ホームゲートウェイ８１０２は、これを受信ノード８１０１にフォワードする（ステップＳ８３１３）。送信ノード８１０１は、これをホームゲートウェイ８１０１から発行された認証要求であると解釈する。

【０２１９】これと同様の手順を双方向に組み、送信ノード８１０１と受信ノード８１０４間で認証手続きが行われる（ステップＳ８３１４）。この間、ホームゲートウェイは、この手続きのバケットを中身を変更せずにフォワードする。認証と並行して、鍵情報のやり取りを行い、受信ノード８１０４は鍵の入手を行い、結局、暗号化されたＭＰＥＧ２映像の復号化ができるようになる。

【０２２０】しかして、送信ノード８１０１が送信するＭＰＥＧ映像を、コンテンツキーＫを使って暗号化し、これが１３９４バスの同期チェネル＃ｘ、ホームゲートウェイ８１０２、公衆網、ホームゲートウェイ８１０３、１３９４バスの同期チェネル＃ｙという経路を辿って、受信ノード８１０３に到達する（ステップＳ８３１５～Ｓ８３１７）。そして、受信ノード８１０３では、暗号化されたＭＰＥＧ映像は、暗号鍵Ｋを使って暗号復号化され、デコードされて、再生表示される。

【０２２１】このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイを介して、送信ノードと受信ノードが認証手続きや鍵交換手続きを行うことで、実際のＭＰＥＧ映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２２２】なお、第５の実施形態において、公衆網の通信帯域が十分に広くない場合には、両ホームゲートウェイにおいて第４の実施形態の符号化変換（例えば、ホームゲートウェイ８１０２ではＭＰＥＧ２／ＭＰＥＧ４変換、ホームゲートウェイ８１０３ではＭＰＥＧ４／ＭＰＥＧ２変換）を行うことによって、若干の圧縮損はあるものの、両家庭網間でコピープロテクションを考慮したデータ転送を行うことが可能になる。

【０２２３】（第６の実施形態）第１の実施形態においては、中継ノードがＩＥＥＥ１３９４バスと無線網との両方に接続され、ＩＥＥＥ１３９４バス上の送信ノードと無線網上の無線ノードとの間で暗号化された映像データのやり取りをする場合の、認証・鍵交換方式を説明した。第１の実施形態では、認証フォーマットの交換等に代表される実際の認証・鍵交換は、送信ノードと無線ノード間で直接行ない、中継ノードは、これらのデータを透過的に中継する形で、これを実現してきた。

【０２２４】これに対し、第６の実施形態では、第２の実施形態のように、認証・鍵交換の単位を送信ノードと中継ノード間、および中継ノードと無線ノード間でそれぞれ行なう。ただし、第２の実施形態と異なり、中継ノ

ードにてコンテンツデータの暗号の復号化、および再暗号化を行なう必要が無いような方法の説明を行なう。すなわち、第２の実施形態では、到着したデータについて、中継ノードにてＩＥＥＥ１３９４区間の暗号の復号化を行い、無線区間の暗号化を再度行なうといった手順を使っていたが、これに対し、第６の実施形態では、ＩＥＥＥ１３９４バス側から到着した暗号化データをそのまま無線網上に転送できるような方法である。

【０２２５】図７７に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第２の実施形態と同様である。

【０２２６】図７８に、送信ノード９１０１の内部構造の一例を示す。これも第２の実施形態と基本的には同様である。認証フォーマットＡｃｅｒｔが、ノードに一つ用意されている。

【０２２７】図７９に、中継ノード９１０２の内部構造の一例を示す。認証フォーマットＢｃｅｒｔ、Ｃｃｅｒｔが、ネットワークインタフェース毎に一つ（ＩＥＥＥ１３９４側にＢｃｅｒｔ、無線網側にＣｃｅｒｔ）用意されている。ＩＥＥＥ１３９４側のＩＳＯ信号送受信部９２０３と無線ＩＳＯ信号送受信部９２０６間で、（復号化／再暗号化のプロセスを経ずに）直接暗号化されたストリーム信号がやり取りされる点を除いて、第２の実施形態と同様である。

【０２２８】図８０に、無線ノード９１０３の内部構造の一例を示す。これも第２の実施形態と基本的には同様である。認証フォーマットＤｃｅｒｔが、ノードに一つ用意されている。

【０２２９】これまでの実施形態と同様に、中継ノードでは、ＩＥＥＥ１３９４側には無線網上のサービスの、無線網側にはＩＥＥＥ１３９４上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

【０２３０】次に、本実施形態の全体のシーケンス例を図８１に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス（映像送信サブユニット）を代理で無線網側に広告しており、無線ノード（の映像デコードサブユニット）が、中継ノードの代理機能に対してサービス（ＭＰＥＧ映像転送要求）を要求、中継ノードが実際のサービスを提供している送信ノードの映像送信サブユニットに対して、実際の映像転送要求を行う。実際の映像データは、暗号化された形でＩＥＥＥ１３９４上は同期チャネル＃ｘ上を、無線網上は無線同期チャネル＃ｙ上を転送されるものとする。なお、詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

【０２３１】また、送信ノード９１０１の動作手順例を図８２に、中継ノード９１０２の動作手順例を図８３／図８４に、無線ノード９１０３の動作手順例を図８５／図８６に、それぞれ示す。

【０２３２】本実施形態では、ＩＥＥＥ１３９４上の著作権保護方式である「５Ｃ　Ｄｉｇｉｔａｌ　ＴｒａｎｓｍｉｓｓｉｏｎＣｏｎｔｅｎｔ　ＰｒｏｔｏｃｔｉｏｎＳｐｅｃｉｆｉｃａｔｉｏｎ」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。なお、本実施形態では、認証・鍵交換方式をノード単位で行う場合について説明する（サブユニット単位で行う場合については、第７の実施形態で説明する）。

【０２３３】さて、送信ノード９１０１は、ＩＥＥＥ１３９４の同期チャネル＃ｘ上に、コンテンツ鍵Ｋで暗号化されたＭＰＥＧ映像を転送する（ステップＳ８５０１，Ｓ８６０１，Ｓ８７０１）。これを受信した中継ノード９１０２は、このまま（受信したＭＰＥＧ映像を、コンテンツ鍵Ｋで暗号化されたまま）無線網側の無線同期チャネル＃ｙに対して転送する（ステップＳ８５０９，Ｓ８７０１）。

【０２３４】同期チャネル＃ｙを通して受信したデータが暗号化されていると認識した中継ノード９１０２は、到着したデータのＣＩＰヘッダの送信ノードＩＤフィールド（ＳＩＤフィールド）を参照する等して、送信ノード９１０１と認証・鍵交換すべきであると認識する（ステップＳ８８０１）。中継ノード９１０２の認証フォーマットＢｃｅｒｔを含んだ認証要求パケットを送信ノード９１０１に対して転送する（ステップＳ８５０２，Ｓ８７０２）。

【０２３５】これを受信した送信ノード９１０１は、送信ノードの認証フォーマットＡｃｅｒｔを含んだ認証要求パケットを中継ノード９１０２に対して送信する（ステップＳ８５０３，Ｓ８６０２，Ｓ８６０３，Ｓ８７０３）。

【０２３６】次に、認証・鍵交換手続きを行って、送信ノード９１０１と中継ノード９１０２の両者で、認証鍵Ｋａｕｔｈ１を秘密裏に共有する（ステップＳ８５０４，Ｓ８５０５，Ｓ８６０４，Ｓ８７０４）。

【０２３７】ＩＥＥＥ１３９４著作権保護方式では、コンテンツ鍵Ｋは、交換鍵Ｋｘ、シードＮｃ、暗号制御情報ＥＭＩの３つの変数の関数Ｊにて計算される。すなわち、Ｋ＝Ｊ（Ｋｘ，Ｎｃ、ＥＭＩ）である。ここでＥＭＩは転送される暗号化データには必ず付与される値である。よって、送信ノード９１０１は、受信側（中継ノード、本実施形態の場合は無線ノードも）に対して、交換鍵ＫｘとシードＮｃの値を通知する必要がある。

【０２３８】そこで、送信ノード９１０１は、中継ノード９１０２との間で共有した認証鍵Ｋａｕｔｈ１を使って、既知の関数ｆを使って、ｆ（Ｋｘ，Ｋａｕｔｈ）の形で中継ノード９１０２に送信する（ステップＳ８５０６，Ｓ８６０５，Ｓ８７０８，Ｓ８７０９）。中継ノード９１０２は、この値から、Ｋｘの値を算出することができる。同様に、シードＮｃの値も、送信ノード９１０１から中継ノード９１０２に転送される（ステップＳ８

５０７，Ｓ８６０６，Ｓ８７１０）。ここで、中継ノード９１０２は、暗号を復号するコンテンツ鍵Ｋを生成するのに必要なＫｘ，Ｎｃの値をこの時点で認識したことになる。

【０２３９】さて、同様の手続きが中継ノード９１０２と無線ノード９１０３の間でも行われる（ステップＳ８５１０～Ｓ８５１３，Ｓ８７０５～Ｓ８７０７，Ｓ８８０２～Ｓ８８０４）。この手続きは、送信ノード９１０１と中継ノード９１０２との間の認証・鍵交換手続きと同様であるので、ここでの詳細な説明は省略する。ここで、無線網の無線同期チャネル＃ｙ上を転送される暗号化されたデータにも、送信元ノードである中継ノード９１０２を識別できるようなアドレス情報等が付与されていてもよい。

【０２４０】さて、中継ノード９１０２と無線ノード９１０１とで認証鍵Ｋａｕｔｈ２が共有できたものとする。本実施形態では、中継ノード９１０２は、暗号化されたＭＰＥＧ映像を暗号の復号化をすることなく、そのまま無線網（の無線同期チャネル＃ｙ）にフォワード処理を行ってしまうため、中継ノード９１０２は無線ノード９１０３に対して、ＩＥＥＥ１３９４区間と同じ交換鍵ＫｘとシードＮｃの値を通知する必要がある（逆に通知できれば、無線ノード９１０３は暗号の復号化が可能である。ただし、ＩＥＥＥ１３９４区間と無線網区間は、同じコンテンツ保護ポリシーで運営されているものとする）。そこで、中継ノード９１０２は、Ｓ８５０６、Ｓ８５０７で受信したデータより算出したＫｘ，Ｎｃのそれぞれの値を、同様に無線ノード９１０３に対して送信する（ステップＳ８５１４，Ｓ８５１５，Ｓ８７０９，Ｓ８７１１，Ｓ８８０５～Ｓ８８０７）。具体的には、Ｋｘの値は認証鍵Ｋａｕｔｈ２の値を使ってｆ（Ｋｘ，Ｋａｕｔｈ２）を計算して、無線ノード９１０３に送出し、Ｎｃの値はそのまま転送する。

【０２４１】無線ノード９１０３では、このようにして、中継ノードと同じ手順を使ってＫｘ、Ｎｃの値を認識できるため、同様の関数Ｊを使ってコンテンツ鍵Ｋの値を算出することができる（ステップＳ８５１６）。

【０２４２】よって、送信ノード９１０１から送られてくる、コンテンツ鍵Ｋで暗号化されたＭＰＥＧ映像は、中継ノード９１０２で暗号の復号化がなされず、そのままフォワードして無線ノード９１０３まで転送されてきた場合（ステップＳ８５０８，Ｓ８５１７，Ｓ８６０７，Ｓ８７１２，Ｓ８８０９）でも、先にＳ８５１６で計算したコンテンツ鍵Ｋの値を使って、暗号の復号化ができる（ステップＳ８５１８，Ｓ８８１０）。その後、ＭＰＥＧ映像のデコード、ディスプレイ表示等が行われる。

【０２４３】なお、本実施形態では、無線網上では無線同期チャネルが定義されており、暗号化されたＭＰＥＧ映像はこの無線同期チャネル上を転送されてくるとして説明を行ってきたが、第２の実施形態のように、無線網上でのＱＯＳデータ転送がイーサネットと同様の無線フレームを転送する場合にも、同様の方法（Ｋｘ，Ｎｃの値を中継ノードから無線ノードにフォワードする）が適用可能である。

【０２４４】逆に言うと、本実施形態のような方法により、中継ノード９１０２では暗号の復号化および再暗号化が不要になり、高速なパケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

【０２４５】なお、この場合、ＩＥＥＥ１３９４側に送信ノード９１０２とは別のノード（別ノード）が存在しており、この別ノードから中継ノード９１０２を経て、無線ノード９１０３に別のコンテンツ鍵で暗号化されたデータ（厳密には同じＥＭＩを持ったデータ）を送信することはできない。コンテンツ鍵は、基本的にデータの送信ノード９１０１が決定する仕組みとなっていることから、別ノードが別のコンテンツ鍵を選択する可能性は十分にある。しかし、中継ノード９１０２と無線ノード９１０３との間で、既にコンテンツ鍵Ｋが一意に定義されている。すなわち、中継ノード９１０２と無線ノード９１０３との間では、同じＥＭＩ値については、１つのコンテンツ鍵しか共有できない。よって、両ノード間では、高々１つのコンテンツ鍵しか使うことができないため、別ノードからの（別のコンテンツ鍵で暗号化された）データを受信しても、これを中継ノード９１０２から無線ノード９１０３に転送する際に、別のコンテンツ鍵を生成できないため、これを復号化できないことになる。

【０２４６】よって、中継ノード９１０２は、既に暗号化データを送信しているノード（本実施形態の場合、無線ノード９１０３）に対して、別のコンテンツ鍵を使う必要のある暗号化データの送信要求があった場合（例えば、ＩＥＥＥ１３９４の別ノードの代理サービスに対するサービス要求があった場合等）は、これを拒否することにより、未然に上記矛盾を回避することが可能となる。また、中継ノード９１０２は、既に無線ノード９１０３に対して暗号化データの送信を行っている場合には、該無線ノード９１０３に対しては、他のサービス（サブユニット）は見せない（代理サービス提供自体を中断する、あるいは暗号化ストリーム転送を伴う代理サービスの提供を中断する、等）、というやり方でも、同様の効果が考えられる。

【０２４７】（第７の実施形態）第６の実施形態では、認証・鍵交換の単位を送信ノードと中継ノードとの間、および中継ノードと無線ノードとの間でそれぞれ行ない、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いような方法であった。

【０２４８】これに対し、第７の実施形態では、中継ノードにて暗号の復号化、および再暗号化を行なう必要が無いのは同様であるが、無線網側での認証・鍵交換の単

位が、第２の実施形態と同じくサブユニット単位にでき、同じノード間でも複数のコンテンツ鍵を持つことができるような場合である。本実施形態によれば、ＩＥＥＥ１３９４上の複数送信ノードからの暗号化データの同時受信が可能となる。

【０２４９】図８７に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は、送信ノード（ＰとＱ）が２つある点以外、基本的には第６の実施形態と同様である。

【０２５０】送信ノード９８０１，９８１１の内部構成は、第６の実施形態と同様である。

【０２５１】中継ノード９８０２の内部構成は、ＩＥＥＥ１３９４側では認証・鍵交換の単位がノード間であり、無線網側では認証・鍵交換の単位がサブユニット間である点を除いて、第６の実施形態と同様である。

【０２５２】無線ノード９８０３の内部構成は、認証・鍵交換の単位がサブユニット間である点を除いて、第６の実施形態と同様である。

【０２５３】なお、送信ノード９８０１，９８１１、無線ノード９８０２の動作手順は基本的には第６の実施形態と同様である。また、１つの送信ノードに対して中継を行う場合の中継ノード９８０３の動作手順も基本的には第６の実施形態と同様である。

【０２５４】これまでの実施形態と同様に、中継ノードでは、ＩＥＥＥ１３９４側には無線網上のサービスの、無線網側にはＩＥＥＥ１３９４上のサービスのそれぞれ代理サービス機能があるものとする。なお、ここでの詳細な説明は省略する。

【０２５５】次に、複数の送信ノードに対して中継を行う場合の中継ノード９８０２の動作手順例を図８８に、本実施形態の全体のシーケンス例を図８９／図９０に示す。これまでの実施形態と同様に、例えば中継ノードが、送信ノードが提供しているサービス（映像送信サブユニット）を代理で無線網側に広告しており、無線ノード（の映像デコードサブユニット）が、中継ノードの代理機能に対してサービス（ＭＰＥＧ映像転送要求）を要求、中継ノードが実際のサービスを提供している送信ノードの映像送信サブユニットに対して、実際の映像転送要求を行う。実際の映像データは、暗号化された形でＩＥＥＥ１３９４上は同期チャネル＃ｘ上を、無線網上は無線同期チャネル＃ｙ上を転送されるものとする。詳細はこれまでの実施形態と同様であるので、ここでの詳細な説明は省略する。

【０２５６】本実施形態でも、ＩＥＥＥ１３９４上の著作権保護方式である「５Ｃ Ｄｉｇｉｔａｌ Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｅｎｔ ＰｒｏｔｏｃｔｉｏｎＳｐｅｃｉｆｉｃａｔｉｏｎ」の認証・鍵交換方式に基本的に準ずる手順を踏むものとする。

【０２５７】さて、送信ノードＰ（９８０１）は、ＩＥＥＥ１３９４の同期チャネル＃ｘ上に、コンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像を転送する（ステップＳ９２０１，Ｓ９３０１）。第６の実施形態と同様に、コンテンツ鍵Ｋｌは、Ｋｌ＝Ｊ（Ｋｘｐ，Ｎｃｐ，ＥＭＩ）にて計算されるものとする。これを受信した中継ノード９８０２は、このまま（受信したＭＰＥＧ映像を、コンテンツ鍵Ｋ１で暗号化されたまま）無線網側の無線同期チャネル＃ｙに対して転送する（ステップＳ９２０９，Ｓ９３０１）。

【０２５８】中継ノード９８０２が送信ノードＰに対して認証要求をし、鍵交換などを行って、交換鍵ＫｘｐとシードＮｃｐを獲得する手順（ステップＳ９２０２～Ｓ９２０７，Ｓ９３０２）は、第６の実施形態と同様であるので、ここでの詳細な説明は省略する。この時点で、中継ノード９８０２は暗号を復号するために必要なＫｘｐ，Ｎｃｐの値を認識したことになる。

【０２５９】さて、同様の認証・鍵交換手続きが中継ノード９８０２と無線ノード９８０３の間でも行われる（ステップＳ９２１０～Ｓ９２１７，Ｓ９３０３）。この手続きは第２の実施形態の送信ノードと中継ノード間の認証・鍵交換手続きと同様であるので、ここでの詳細な説明は省略する。ただし、認証先問い合わせや認証先応答、あるいは認証要求にサブユニットのＩＤの他、チャネル番号、あるいは暗号化データの送受信を行うことになるプラグの識別子を搭載して、これを行ってもよい。中継ノード９８０２、あるいは無線ノード９８０３が、「どの暗号化データについての認証・鍵交換手続きか」ということが識別できるようになり、後述するように、異なる鍵の暗号化データについては、同一のノード間の認証・鍵交換であったとしても、異なる鍵を通知することが可能になる。

【０２６０】なお、この際、認証要求にチャネル番号を含める場合は、ステップＳ９２１０の認証先問い合わせとステップＳ９２１１の認証先応答は不要となる。

【０２６１】さて、中継ノード９８０２と無線ノード９８０３で認証鍵Ｋａｕｔｈｌが共有できたものとする。本実施形態でも、中継ノード９８０２は、暗号化されたＭＰＥＧ映像を暗号の復号化をすることなく、そのまま無線網（の無線同期チャネル＃ｙ）にフォワード処理を行ってしまうため、中継ノード９８０２は無線ノード９８０３に対して、交換鍵ＫｘｐとシードＮｃｐの値を通知する必要がある（逆に通知できれば、無線ノード９８０３は暗号の復号化が可能である）。そこで、中継ノード９８０２は、Ｓ９２０６、Ｓ９２０７で受信したデータより算出したＫｘｐ，Ｎｃｐのそれぞれの値を、同様に無線ノード９８０３に対して送信する（ステップＳ９２１６，Ｓ９２１７）。Ｋｘｐの値は認証鍵Ｋａｕｔｈｌの値を使ってｆ（Ｋｘｐ，Ｋａｕｔｈｌ）を計算して、無線ノード９８０３に送出する（ステップＳ９２１６）。

【０２６２】無線ノード９８０３では、このようにし

て、中継ノード９８０２と同じ手順を使ってＫｘｐ、Ｎｃｐの値を認識できるため、同様の関数Ｊを使ってコンテンツ鍵Ｋ１の値を算出することができる（ステップＳ９２１８）。

【０２６３】よって、送信ノードＰから送られてくる、コンテンツ鍵Ｋ１で暗号化されたＭＰＥＧ映像は、中継ノード９８０２で暗号の復号化をせずに、そのままフォワードして無線ノード９８０３まで転送されてきた場合（ステップＳ９２０８，Ｓ９２１９）でも、先にステップＳ９２１８で計算したコンテンツ鍵Ｋ１の値を使って、暗号の復号化ができる（ステップＳ９２２０）。その後、ＭＰＥＧ映像のデコード、ディスプレイ表示等が行われる。

【０２６４】本実施形態のような方法でも、中継ノード９８０２では暗号の復号化、および再暗号化が不要になり、高速なバケット転送も可能になることから、低コストな中継ノードの構築が可能となる。

【０２６５】さて、次に、別の送信ノードＱ（９８１１）が、同時に中継ノード９８０２を介して無線ノード９８０３に対して別のコンテンツ鍵Ｋ２で暗号化されたデータを送信する場合（ステップＳ９２２１，Ｓ９２２９，Ｓ９３０４）を考える。

【０２６６】本実施形態の前半と同様に、送信ノードＱと中継ノード９８０２との間で認証・鍵交換が行われ（ステップＳ９２２２～Ｓ９２２７）、中継ノード９８０２は交換鍵ＫｘｑとシードＮｃｑの値をそれぞれ得ることができる。

【０２６７】本実施形態においては、中継ノード９８０２と無線ノード９８０３との間の認証は、サブユニット間単位であるので、暗号化データの送受が異なるサブユニット間で行われているものとすれば、中継ノード９８０２と無線ノード９８０３との間で複数の認証・鍵交換が可能となる。

【０２６８】すなわち、本実施形態の前半と同様に、中継ノード９８０２と無線ノード９８０３との間で、本実施形態の前半とは異なるサブユニット間で認証・鍵交換を行っていく（ステップＳ９２３０～Ｓ９２３５，Ｓ９３０５）。その上で、中継ノード９８０２は、送信ノードＱと自ノード（中継ノード）９８０２との間の交換鍵ＫｘｑとシードＮｃｑを、無線ノード９８０３にフォワードする（ステップＳ９２３６，Ｓ９２３７，Ｓ９３０５，Ｓ９３０６）。

【０２６９】無線ノード９８０３では、このようにして、Ｋｘｑ、Ｎｃｑの値を認識できるため、同様の関数Ｊを使ってコンテンツ鍵Ｋ２の値を算出することができる（ステップＳ９２３８）。

【０２７０】よって、送信ノードＱから送られてくる、コンテンツ鍵Ｋ２で暗号化されたＭＰＥＧ映像は、中継ノード９８０２で暗号の復号化をせずに、そのままフォワードして無線ノード９８０３まで転送されてきた場合（ステップＳ９２２８，Ｓ９２２９）でも、先にステップＳ９２３８で計算したコンテンツ鍵Ｋ２の値を使って、暗号の復号化ができる（ステップＳ９２４０）。つまり、２つの異なるコンテンツ鍵（本実施形態ではＫ１とＫ２）で暗号化されたＭＰＥＧ映像の同時受信が可能となる。

【０２７１】なお、第６の実施形態と第７の実施形態では、ＩＥＥＥ１３９４と無線網との相互接続を行う場合を例に説明してきたが、インターネット等のその他の網についても適用可能である。

【０２７２】なお、第１～第７の実施形態において例示したデータ転送の方向とは逆の方向にデータ転送する場合（例えば、無線ノードからＩＥＥＥ１３９４上のノードへデータ転送する場合）にも、本発明は適用可能である。

【０２７３】また、第１～第７の実施形態において、無線ノードやＩＥＥＥ１３９４上のノードについては、コンテンツについて送信機能または受信機能の一方に着目して説明したが、無線ノードやＩＥＥＥ１３９４上のノードは、コンテンツについて送信機能と受信機能の両方を備えることも可能である。

【０２７４】また、認証手続きや、鍵交換手続き（コンテンツ鍵共有手続き）は、これまでに例示したものに限定されず、他の種々の方法が用いられる場合にも本発明は適用可能である。

【０２７５】また、以上では、家庭網ネットワークとして実施形態を説明したが、もちろん、本発明は家庭網以外のネットワークにも適用可能である。

【０２７６】なお、以上の各機能は、ソフトウェアとしても実現可能である。

【０２７７】また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【０２７８】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０２７９】

【発明の効果】本発明によれば、同じネットワークでは接続されていない装置間で、保護すべきコンテンツの送受信のためのコンテンツ保護手続きを行うことが可能になる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態に係るネットワークの全体構成の一例を示す図

【図２】送信ノードの内部構造の一例を示す図

【図３】中継ノードの内部構造の一例を示す図

【図４】無線ノードの内部構造の一例を示す図

【図５】全体のシーケンスの一例を示す図
【図６】全体のシーケンスの一例を示す図
【図７】送信ノードの動作手順の一例を示すフローチャート
【図８】送信ノードの動作手順の一例を示すフローチャート
【図９】中継ノードの動作手順の一例を示すフローチャート
【図１０】中継ノードの動作手順の一例を示すフローチャート
【図１１】中継ノードの動作手順の一例を示すフローチャート
【図１２】無線ノードの動作手順の一例を示すフローチャート
【図１３】無線ノードの動作手順の一例を示すフローチャート
【図１４】無線ノード構成情報パケットの一例を示す図
【図１５】代理テーブルの一例を示す図
【図１６】代理テーブルの一例を示す図
【図１７】送信ノードから見た中継ノードの内部構造を説明するための図
【図１８】無線ノードから見た中継ノードの内部構造を説明するための図
【図１９】無線ノード制御パケットの一例を示す図
【図２０】本発明の第２の実施形態に係るネットワークの全体構成の一例を示す図
【図２１】送信ノードの内部構造の一例を示す図
【図２２】中継ノードの内部構造の一例を示す図
【図２３】無線ノードの内部構造の一例を示す図
【図２４】全体のシーケンスの一例を示す図
【図２５】全体のシーケンスの一例を示す図
【図２６】送信ノードの動作手順の一例を示すフローチャート
【図２７】送信ノードの動作手順の一例を示すフローチャート
【図２８】中継ノードの動作手順の一例を示すフローチャート
【図２９】中継ノードの動作手順の一例を示すフローチャート
【図３０】中継ノードの動作手順の一例を示すフローチャート
【図３１】中継ノードの動作手順の一例を示すフローチャート
【図３２】無線ノードの動作手順の一例を示すフローチャート
【図３３】無線ノードの動作手順の一例を示すフローチャート
【図３４】代理テーブルの一例を示す図
【図３５】代理テーブルの一例を示す図
【図３６】送信ノードから見た中継ノードの内部構造を説明するための図
【図３７】無線ノードから見た中継ノードの内部構造を説明するための図
【図３８】無線フレームのフォーマットの一例を示す図
【図３９】無線制御パケットのフォーマットの一例を示す図
【図４０】本発明の第３の実施形態に係るネットワークの全体構成の一例を示す図
【図４１】送信ノードの内部構造の一例を示す図
【図４２】中継ノードの内部構造の一例を示す図
【図４３】無線ノードの内部構造の一例を示す図
【図４４】全体のシーケンスの一例を示す図
【図４５】全体のシーケンスの一例を示す図
【図４６】送信ノードの動作手順の一例を示すフローチャート
【図４７】送信ノードの動作手順の一例を示すフローチャート
【図４８】中継ノードの動作手順の一例を示すフローチャート
【図４９】中継ノードの動作手順の一例を示すフローチャート
【図５０】中継ノードの動作手順の一例を示すフローチャート
【図５１】無線ノードの動作手順の一例を示すフローチャート
【図５２】無線ノードの動作手順の一例を示すフローチャート
【図５３】代理テーブルの一例を示す図
【図５４】代理テーブルの一例を示す図
【図５５】送信ノードから見た中継ノードの内部構造を説明するための図
【図５６】無線ノードから見た中継ノードの内部構造を説明するための図
【図５７】無線ノードに送られてきた制御画面の一例を示す図
【図５８】本発明の第４の実施形態に係るネットワークの全体構成の一例を示す図
【図５９】送信ノードの内部構造の一例を示す図
【図６０】ホームゲートウェイの内部構造の一例を示す図
【図６１】受信ノードの内部構造の一例を示す図
【図６２】全体のシーケンスの一例を示す図
【図６３】全体のシーケンスの一例を示す図
【図６４】送信ノードの動作手順の一例を示すフローチャート
【図６５】送信ノードの動作手順の一例を示すフローチャート
【図６６】ホームゲートウェイの動作手順の一例を示すフローチャート
【図６７】ホームゲートウェイの動作手順の一例を示す

フローチャート
【図６８】ホームゲートウェイの動作手順の一例を示すフローチャート
【図６９】ホームゲートウェイの動作手順の一例を示すフローチャート
【図７０】受信ノードの動作手順の一例を示すフローチャート
【図７１】受信ノードの動作手順の一例を示すフローチャート
【図７２】送信ノードのパネルとホームゲートウェイの送信ノード制御用ホームページの一例を示す図
【図７３】本発明の第５の実施形態に係るネットワークの全体構成の一例を示す図
【図７４】ホームゲートウェイの内部構造の一例を示す図
【図７５】全体のシーケンスの一例を示す図
【図７６】制御画面の一例を示す図
【図７７】本発明の第６の実施形態に係るネットワークの全体構成の一例を示す図
【図７８】送信ノードの内部構造の一例を示す図
【図７９】中継ノードの内部構造の一例を示す図
【図８０】無線ノードの内部構造の一例を示す図
【図８１】全体のシーケンスの一例を示す図
【図８２】送信ノードの動作手順の一例を示すフローチャート
【図８３】中継ノードの動作手順の一例を示すフローチャート
【図８４】中継ノードの動作手順の一例を示すフローチャート
【図８５】無線ノードの動作手順の一例を示すフローチャート
【図８６】無線ノードの動作手順の一例を示すフローチャート
【図８７】本発明の第７の実施形態に係るネットワークの全体構成の一例を示す図
【図８８】中継ノードの動作手順の一例を示すフローチャート
【図８９】全体のシーケンスの一例を示す図
【図９０】全体のシーケンスの一例を示す図
【符号の説明】
１０１，２１０１，４１０１，６１０１，８１０１，９１０１，９８０１，９８１１…送信ノード
１０２，２１０２，４１０２，９１０２，９８０２…中継ノード
１０３，２１０３，４１０３，６１０４，９１０３，９８０３…無線ノード
６１０２，８１０２，８１０３…ホームゲートウェイ
６１０３，８１０４…受信ノード
１０４，２１０４，４１０４，８１０５，８１０７，９１０４，９８０４…ＩＥＥＥ１３９４バス
６１０５，８１０６…公衆網
２０１，２２０１，４２０１，６２０１，８２０１，９１０１…ＩＥＥＥ１３９４インタフェース
２０２，２２０２，４２０２，９２０２…無線インタフェース
２０３，２２０７，４２０３，６２０７，８２０３，９２０７…ＡＶ／Ｃプロトコル処理部
２０４，２２０３，４２０４，６２０３，８２０４，９２０３…ＩＳＯ信号送受信部
２０５，２２０６，４２０５，９２０６…無線ＩＳＯ信号送受信部
２０６，２２０９，４２０６，６２０９，９２０９…１３９４バス構成認識部
２０７，２２１０，４２０７，８２０７，９２１０…代理サブユニット構成部
２０８，２２１４，４２０８，６２１５，９２１４…代理テーブル
２０９，２２１１，４２０９，９２１１…無線区間構成認識部
２１０，４２１０，８２０９…コピープロテクション制御／フォワード部
２２０８，６２０８…ＩＥＥＥ１３９４コピープロテクション処理部
２２１２，９２１２…無線区間コピープロテクション部
８２１１…変換テーブル
２１１，２２１３，４２１１，９２１３…無線ノード制御パケット送受信部
２２０４，６２０４…暗号復号化部
２２０５，６２０５…暗号化部
４２１２…ＨＡＶｉ処理部
４２１３…ＩＥＥＥ１２１２レジスタ
６２０６，８２０５…ＡＶ信号送受信部
６２０２，８２０２…インターネットインタフェース
６２１０，８２０８…代理ホームページ作成部
６２１１，８２１０…ホームページ作成・蓄積部
６２１２…インターネット側プロテクション処理部
６２１３…制御パケット送受信部
６２１４…ＭＰＥＧ２／ＭＰＥＧ４変換部
６２０６…制御パケット処理信部
３０１，２３０１，４３０１，９３０１…無線インタフェース
３０２，２３０２，４３０２，９３０２…無線ノード制御パケット送受信部
３０３，２３０３，４３０３，６３０３，９３０３…コピープロテクション処理部
３０４，２３０４，４３０４，９３０４…無線ＩＳＯ信号送受信部
３０５，２３０５，４３０５，６３０５，９３０５…暗号復号化部
３０６，２３０６，４３０６，６３０６，９３０６…Ｍ

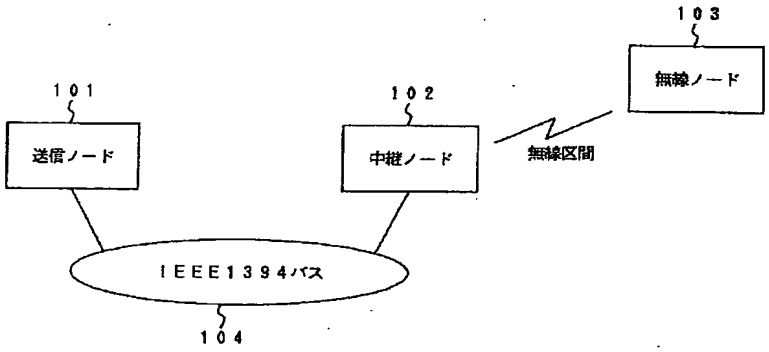
59

ＰＥＧデコード部
３０７，２３０７，４３０７，６３０７，９３０７…ディスプレイ部
６３０１…インターネットインタフェース
６３０２…制御パケット送受信部
６３０４…ＡＶ信号送受信部
４０１，２４０１，４４０１，６４０１，９４０１…ＩＥＥＥ１３９４インタフェース
４０２，２４０２，４４０２，６４０２，９４０２…ＡＶ／Ｃプロトコル処理部

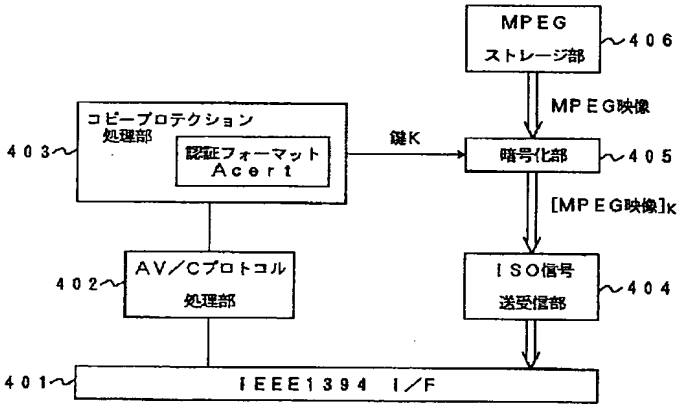
60

＊４０３，２４０３，４４０３，６４０３，９４０３…コピープロテクション処理部
４０４，２４０４，４４０４，６４０４，９４０４…ＩＳＯ信号送受信部
４０５，２４０５，４４０５，６４０５，９４０５…暗号化部
４０６，２４０６，４４０６，６４０６，９４０６…ＭＰＥＧストレージ部
４４０７…ＩＥＥＥ１２１２レジスタ

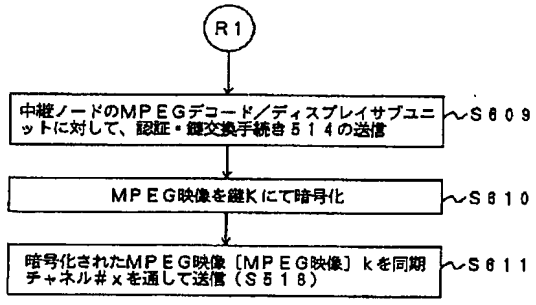
【図１】



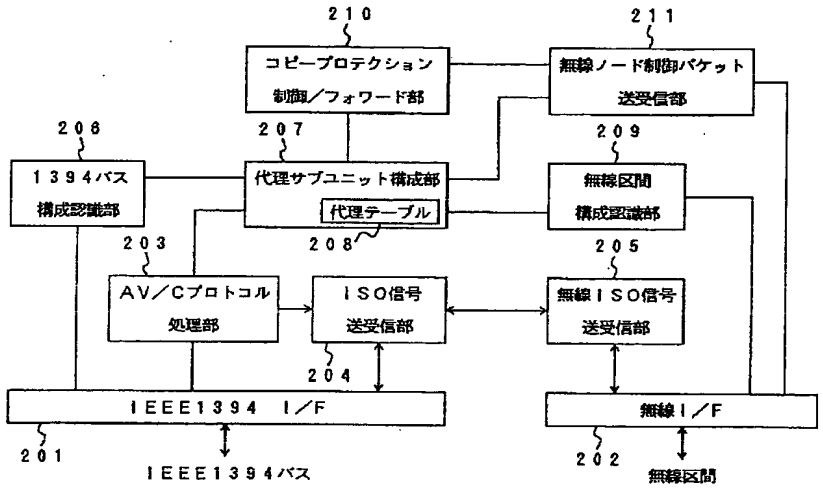
【図２】



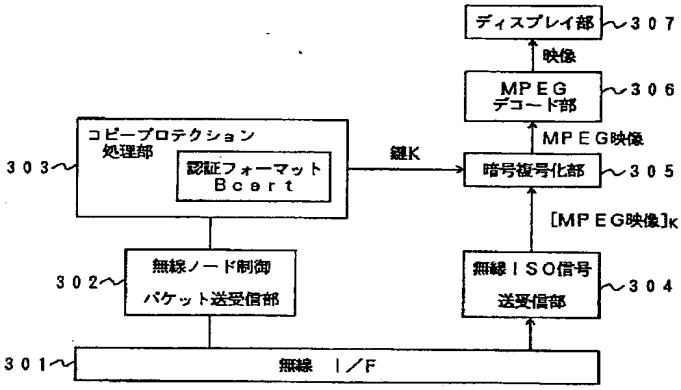
【図８】



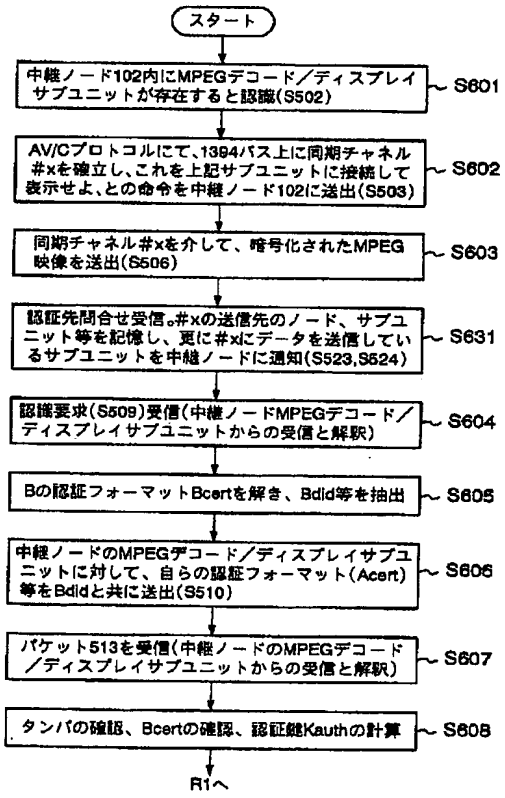
【図３】


２１０
２１１
コピープロテクション
制御／フォワード部
無線ノード制御パケット
送受信部
２０６
２０７
２０９
１３９４バス
構成認識部
代理サブユニット構成部
代理テーブル
無線区間
構成認識部
２０８
２０３
２０５
AV／Cプロトコル
処理部
ＩＳＯ信号
送受信部
無線ＩＳＯ信号
送受信部
２０４
ＩＥＥＥ１３９４　Ｉ／Ｆ
無線Ｉ／Ｆ
２０１
２０２
ＩＥＥＥ１３９４バス
無線区間

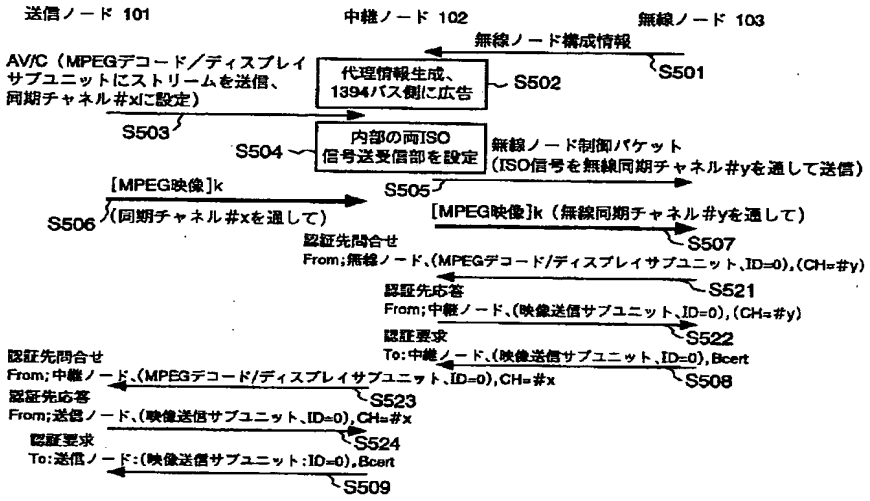
【図４】


ディスプレイ部
３０７
映像
MPEG
デコード部
３０６
コピープロテクション
処理部
認証フォーマット
Bcert
３０３
鍵K
MPEG映像
暗号復号化部
３０５
[MPEG映像]k
無線ノード制御
パケット送受信部
３０２
無線ＩＳＯ信号
送受信部
３０４
３０１
無線　Ｉ／Ｆ

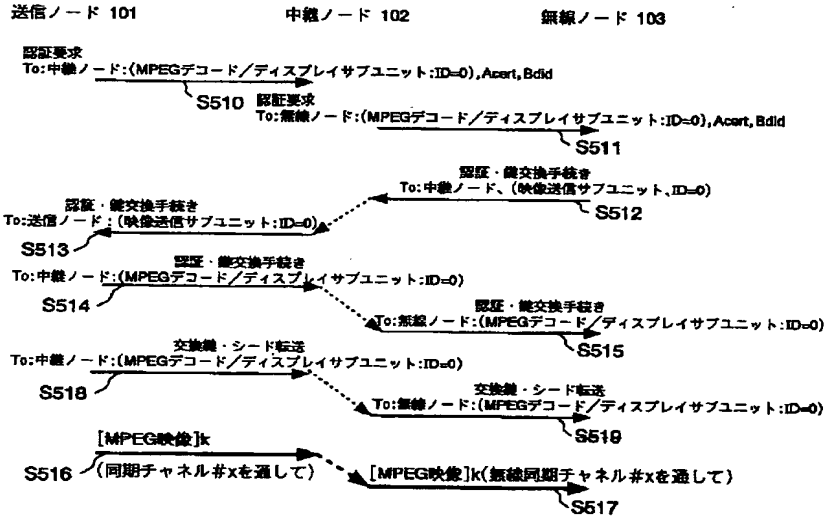
【図７】


スタート
中継ノード102内にMPEGデコード／ディスプレイ
サブユニットが存在すると認識(S502)
S601
AV/Cプロトコルにて、1394バス上に同期チャネル
#xを確立し、これを上記サブユニットに接続して
表示せよ、との命令を中継ノード102に送出(S503)
S602
同期チャネル#xを介して、暗号化されたMPEG
映像を送出(S506)
S603
認証先問合せ受信。#xの送信先のノード、サブユ
ニット等を記憶し、更に#xにデータを送信してい
るサブユニットを中継ノードに通知(S523,S524)
S631
認識要求(S509)受信(中継ノードMPEGデコード／
ディスプレイサブユニットからの受信と解釈)
S604
Bの認証フォーマットBcertを解き、Bdid等を抽出
S605
中継ノードのMPEGデコード／ディスプレイサブユ
ニットに対して、自らの認証フォーマット(Acert)
等をBdidと共に送出(S510)
S606
パケット513を受信(中継ノードのMPEGデコード
／ディスプレイサブユニットからの受信と解釈)
S607
タンパの確認、Bcertの確認、認証鍵Kauthの計算
S608
R1へ

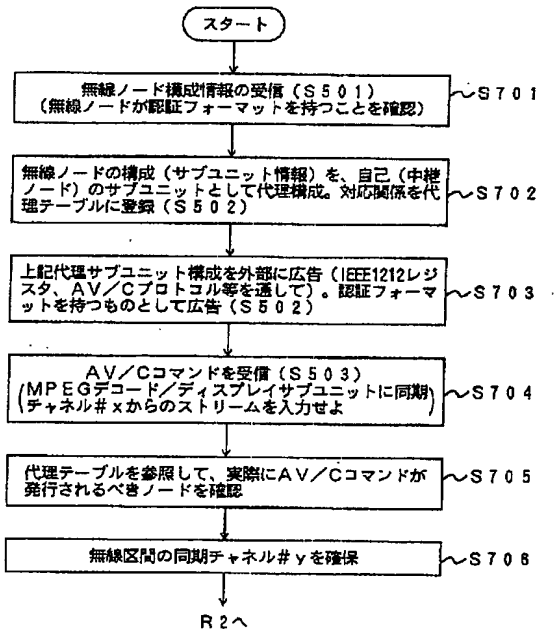
【図５】


送信ノード 101
中継ノード 102
無線ノード 103
無線ノード構成情報
S501
AV/C（MPEGデコード／ディスプレイサブユニットにストリームを送信、同期チャネル#xに設定）
代理情報生成、1394バス側に広告
S502
S503
S504
内部の両ISO信号送受信部を設定
無線ノード制御パケット（ISO信号を無線同期チャネル#yを通して送信）
S505
[MPEG映像]k
S506
（同期チャネル#xを通して）
[MPEG映像]k（無線同期チャネル#yを通して）
S507
認証先問合せ
From;無線ノード、(MPEGデコード/ディスプレイサブユニット、ID=0)、(CH=#y)
S521
認証先応答
From;中継ノード、(映像送信サブユニット、ID=0)、(CH=#y)
S522
認証要求
To:中継ノード、(映像送信サブユニット、ID=0)、Bcert
S508
認証先問合せ
From;中継ノード、(MPEGデコード/ディスプレイサブユニット、ID=0)、CH=#x
S523
認証先応答
From;送信ノード、(映像送信サブユニット、ID=0)、CH=#x
S524
認証要求
To:送信ノード:(映像送信サブユニット:ID=0)、Bcert
S509

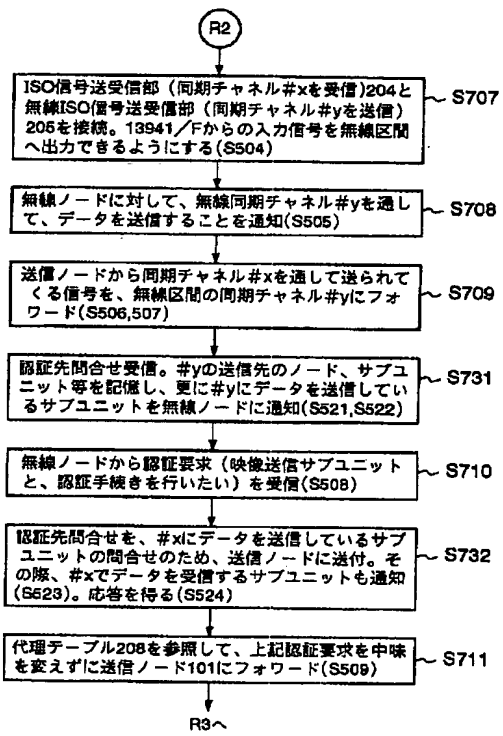
【図６】


送信ノード 101
中継ノード 102
無線ノード 103
認証要求
To:中継ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)、Acert、Bdid
S510
認証要求
To:無線ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)、Acert、Bdid
S511
認証・鍵交換手続き
To:中継ノード、(映像送信サブユニット、ID=0)
S512
認証・鍵交換手続き
To:送信ノード：(映像送信サブユニット:ID=0)
S513
認証・鍵交換手続き
To:中継ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)
S514
認証・鍵交換手続き
To:無線ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)
S515
交換鍵・シード転送
To:中継ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)
S518
交換鍵・シード転送
To:無線ノード:(MPEGデコード／ディスプレイサブユニット:ID=0)
S519
[MPEG映像]k
S516
（同期チャネル#xを通して）
[MPEG映像]k(無線同期チャネル#xを通して)
S517

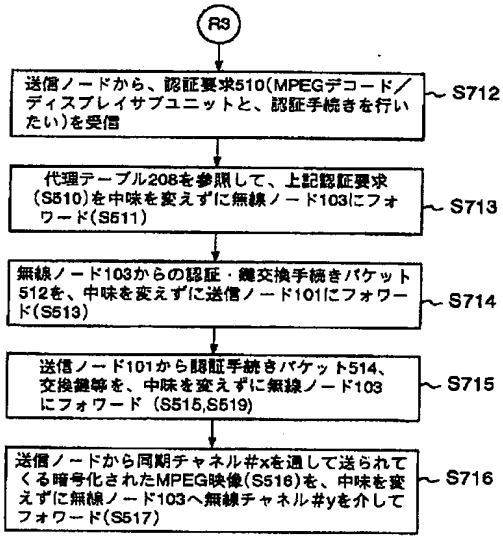
【図９】



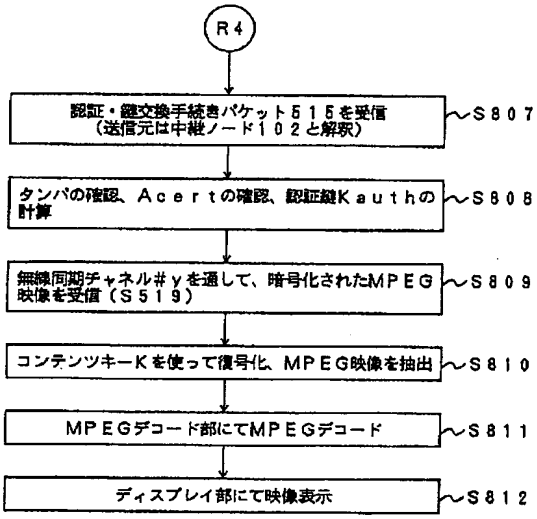
【図１０】



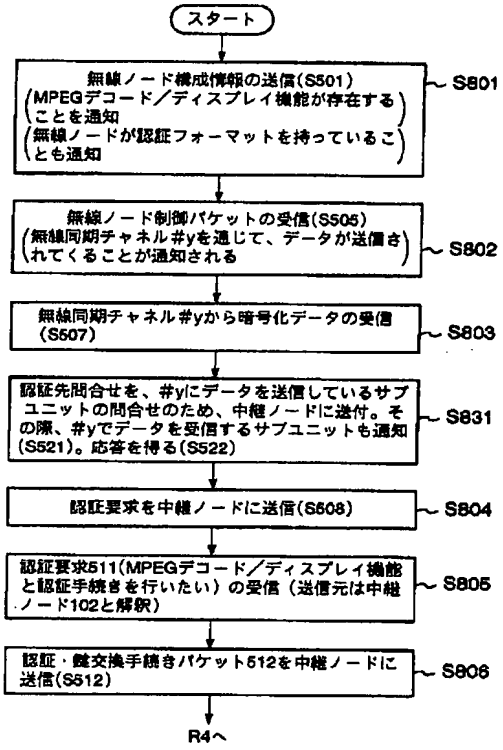
【図１１】



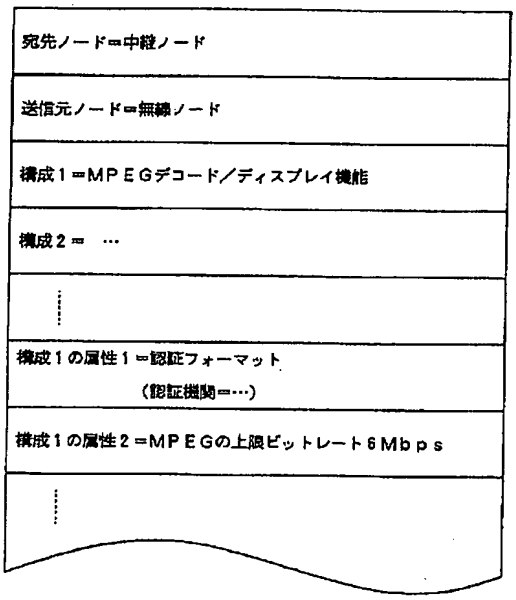
【図１３】



【図１２】



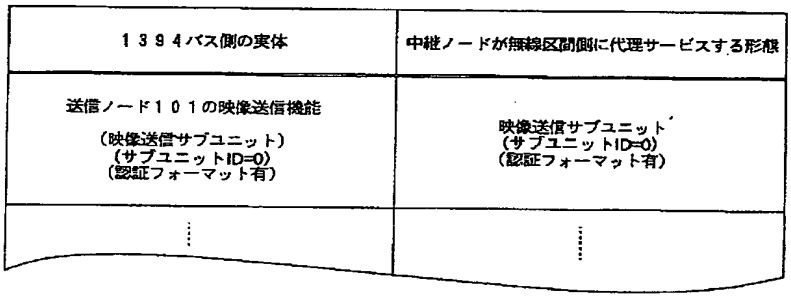
【図１４】



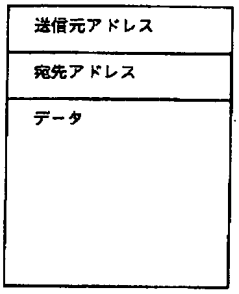
【図１５】

無線区間側の実体	中継ノードが１３９４側に代理サービスする形態
無線ノード１０３の ＭＰＥＧデコード／ディスプレイ機能 (サブユニットID=0) (認証フォーマット有)	ＭＰＥＧデコード／ディスプレイサブユニット (サブユニットID=0) (認証フォーマット有)
⋮	⋮

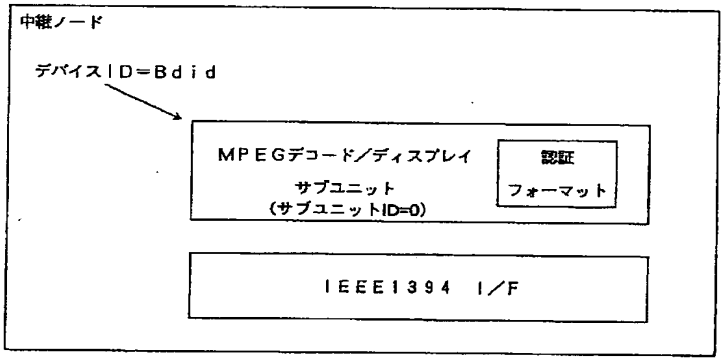
【図１６】



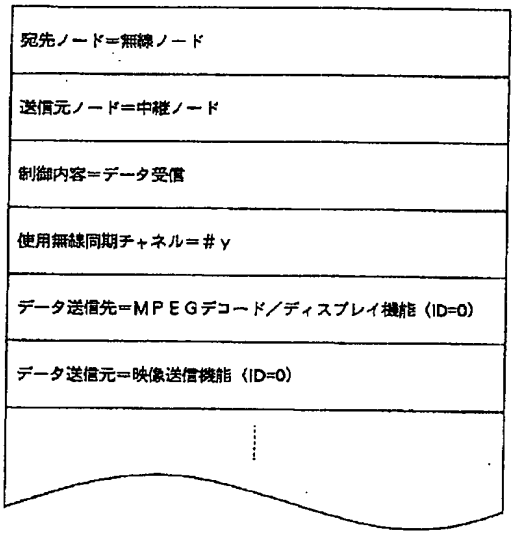
【図３８】



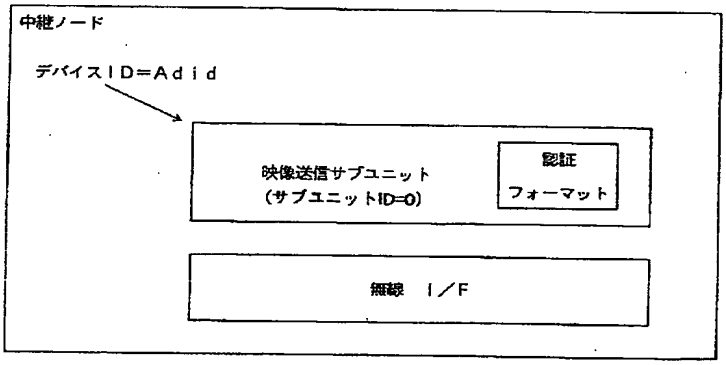
【図１７】



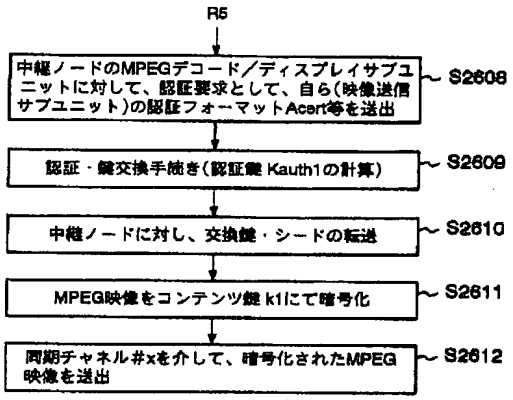
【図１９】



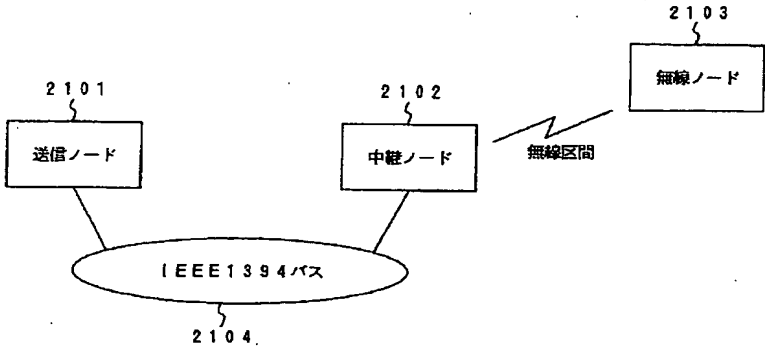
【図１８】



【図２７】



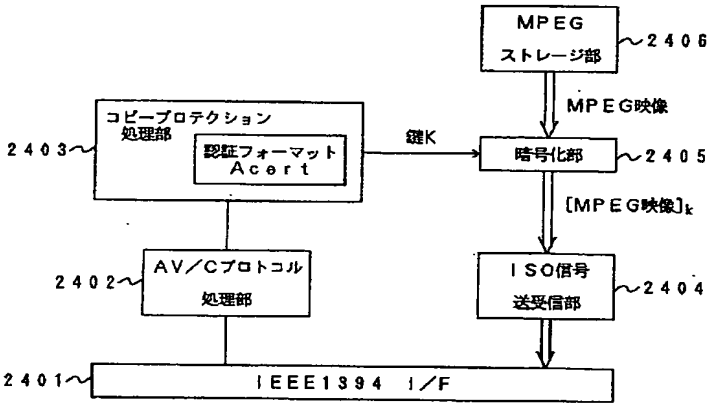
【図２０】



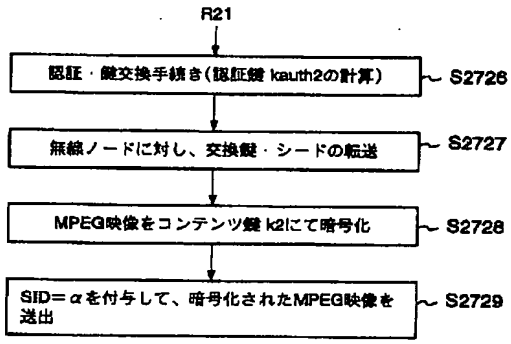
【図３９】

宛先ノード＝無線ノード
送信元ノード＝中継ノード
制御内容＝データ受信
使用SID＝α
データ送信先＝ MPEGデコード／ディスプレイ サブユニット（サブユニットID＝0）
データ送信元＝ 映像送信サブユニット （サブユニットID＝0）

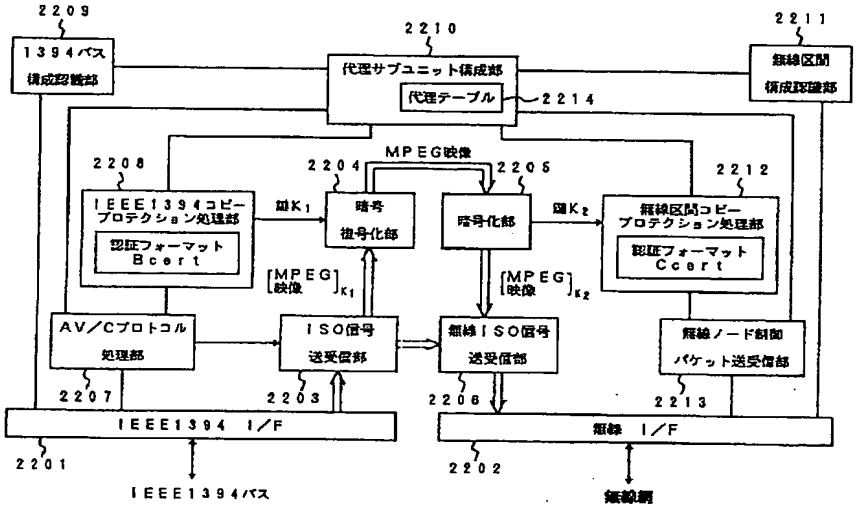
【図２１】



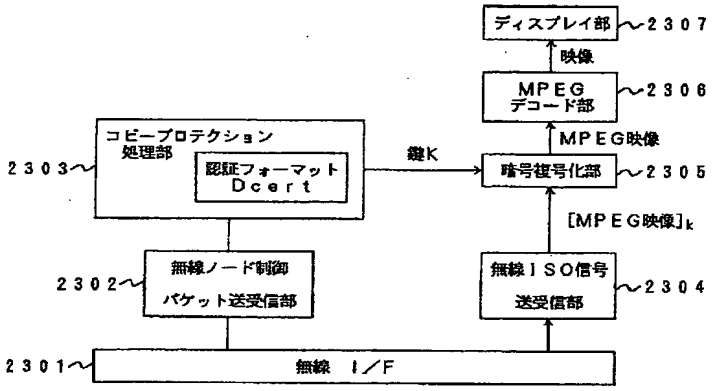
【図３１】



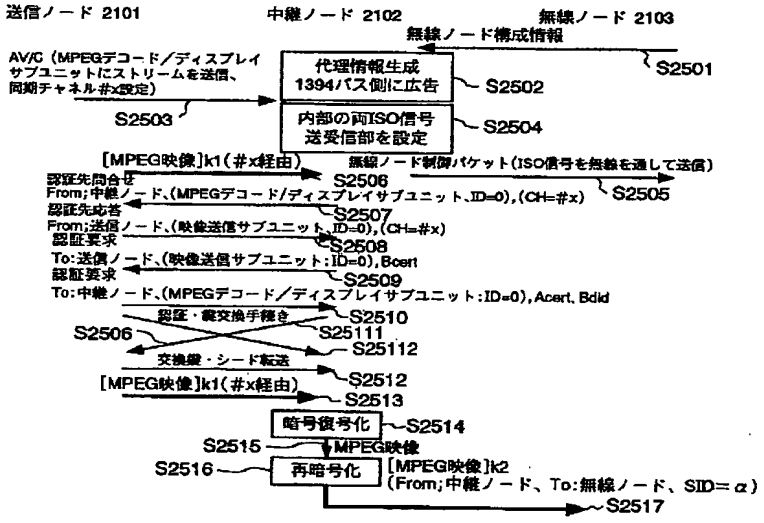
【図２２】



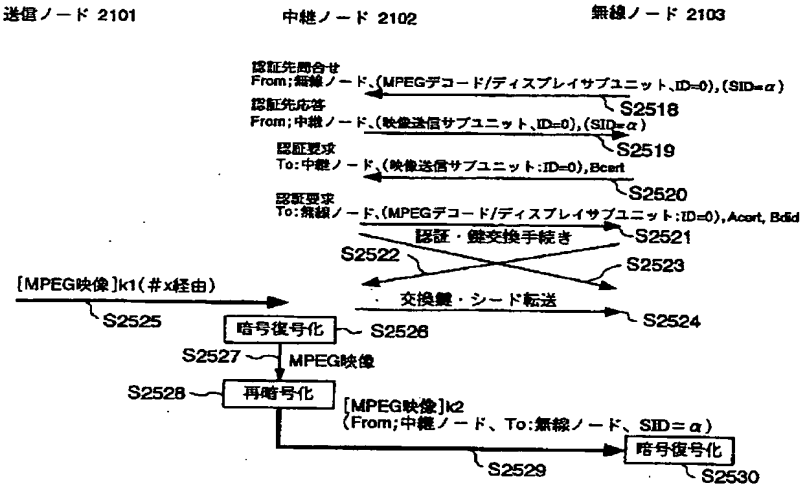
【図２３】


ディスプレイ部
２３０７
映像
MPEG
デコード部
２３０６
MPEG映像
コピープロテクション
処理部
２３０３
認証フォーマット
Dcert
鍵K
暗号復号化部
２３０５
[MPEG映像]k
２３０２
無線ノード制御
パケット送受信部
無線ＩＳＯ信号
送受信部
２３０４
２３０１
無線　Ｉ／Ｆ

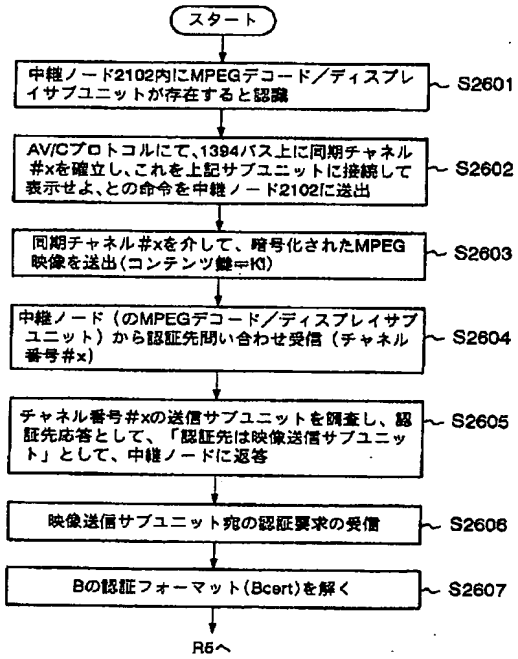
【図２４】


送信ノード 2101
中継ノード 2102
無線ノード 2103
無線ノード構成情報
S2501
AV/C（MPEGデコード/ディスプレイ
サブユニットにストリームを送信、
同期チャネル#x設定）
代理情報生成
1394バス側に広告
S2502
S2503
内部の両ISO信号
送受信部を設定
S2504
[MPEG映像]k1（#x経由）
S2506
無線ノード制御パケット（ISO信号を無線を通して送信）
S2505
認証先問合せ
From;中継ノード、(MPEGデコード/ディスプレイサブユニット、ID=0)、(CH=#x)
S2507
認証先応答
From;送信ノード、(映像送信サブユニット、ID=0)、(CH=#x)
S2508
認証要求
To:送信ノード、(映像送信サブユニット:ID=0)、Bcert
S2509
認証要求
To:中継ノード、(MPEGデコード/ディスプレイサブユニット:ID=0)、Acert、Bdid
S2510
認証・鍵交換手続き
S25111
S2506
S25112
交換鍵・シード転送
[MPEG映像]k1（#x経由）
S2512
S2513
暗号復号化
S2514
S2515
MPEG映像
S2516
再暗号化
[MPEG映像]k2
(From;中継ノード、To:無線ノード、SID＝α)
S2517

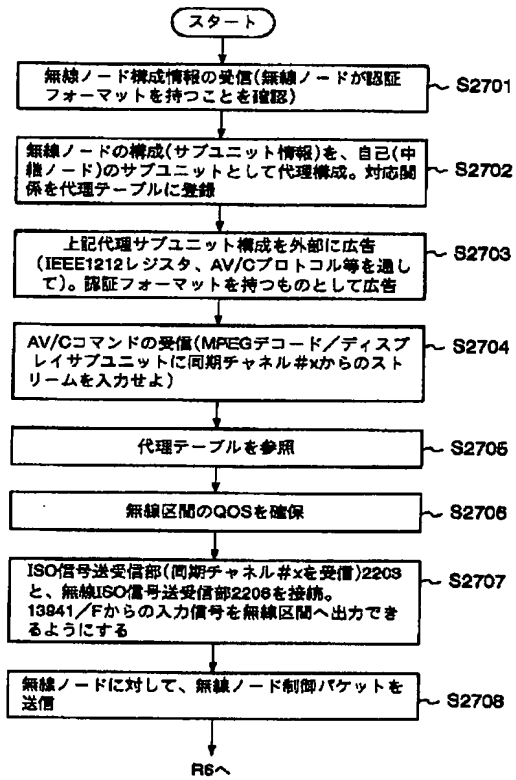
【図２５】


送信ノード 2101
中継ノード 2102
無線ノード 2103
認証先問合せ
From;無線ノード,(MPEGデコード/ディスプレイサブユニット,ID=0),(SID=α)
S2518
認証先応答
From;中継ノード,(映像送信サブユニット,ID=0),(SID=α)
S2519
認証要求
To:中継ノード,(映像送信サブユニット:ID=0),Bcert
S2520
認証要求
To:無線ノード,(MPEGデコード/ディスプレイサブユニット:ID=0),Acert, Bcid
S2521
認証・鍵交換手続き
S2522
S2523
[MPEG映像]k1(#x経由)
S2525
交換鍵・シード転送
S2524
暗号復号化
S2526
S2527
MPEG映像
S2528
再暗号化
[MPEG映像]k2
(From;中継ノード、To:無線ノード、SID＝α)
暗号復号化
S2529
S2530

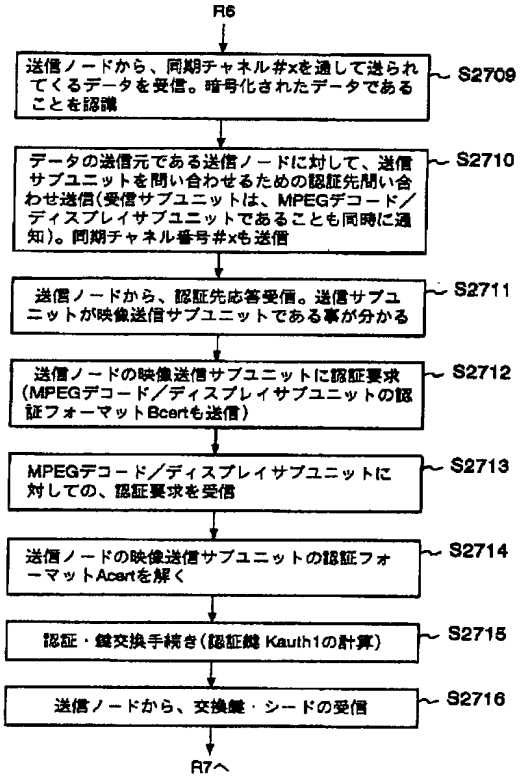
【図２６】


スタート
中継ノード2102内にMPEGデコード／ディスプレイサブユニットが存在すると認識
S2601
AV/Cプロトコルにて、1394バス上に同期チャネル#xを確立し、これを上記サブユニットに接続して表示せよ、との命令を中継ノード2102に送出
S2602
同期チャネル#xを介して、暗号化されたMPEG映像を送出(コンテンツ鍵=K)
S2603
中継ノード（のMPEGデコード／ディスプレイサブユニット）から認証先問い合わせ受信（チャネル番号#x)
S2604
チャネル番号#xの送信サブユニットを調査し、認証先応答として、「認証先は映像送信サブユニット」として、中継ノードに返答
S2605
映像送信サブユニット宛の認証要求の受信
S2606
Bの認証フォーマット(Bcert)を解く
S2607
R5へ

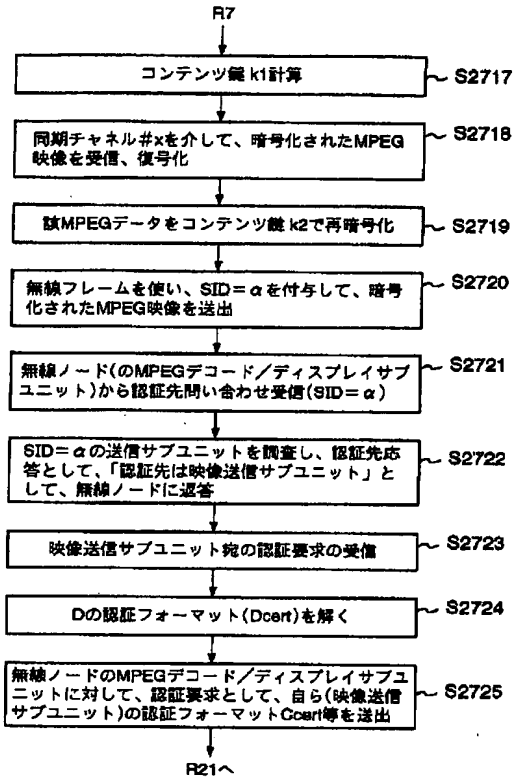
【図２８】


スタート
無線ノード構成情報の受信(無線ノードが認証フォーマットを持つことを確認)
S2701
無線ノードの構成(サブユニット情報)を、自己(中継ノード)のサブユニットとして代理構成。対応関係を代理テーブルに登録
S2702
上記代理サブユニット構成を外部に広告(IEEE1212レジスタ、AV/Cプロトコル等を通して)。認証フォーマットを持つものとして広告
S2703
AV/Cコマンドの受信(MPEGデコード／ディスプレイサブユニットに同期チャネル#xからのストリームを入力せよ)
S2704
代理テーブルを参照
S2705
無線区間のQOSを確保
S2706
ISO信号送受信部(同期チャネル#xを受信)2203と、無線ISO信号送受信部2206を接続。1394／Fからの入力信号を無線区間へ出力できるようにする
S2707
無線ノードに対して、無線ノード制御パケットを送信
S2708
R6へ

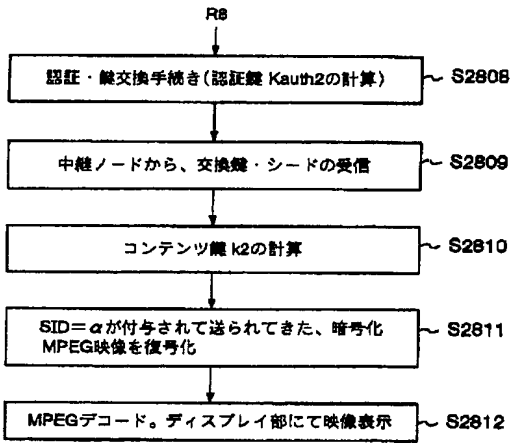
【図２９】



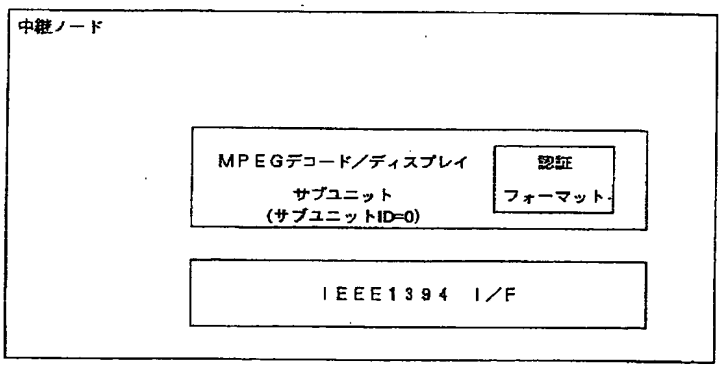
【図３０】



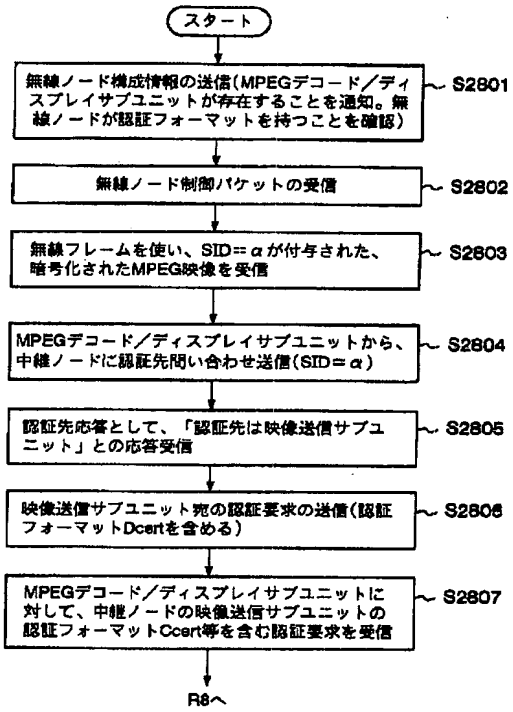
【図３３】



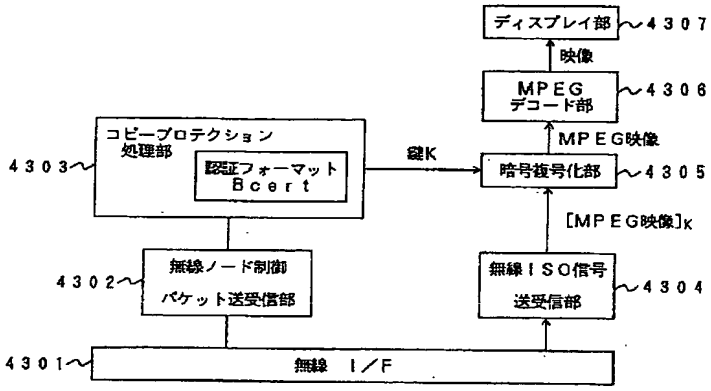
【図３６】



【図３２】



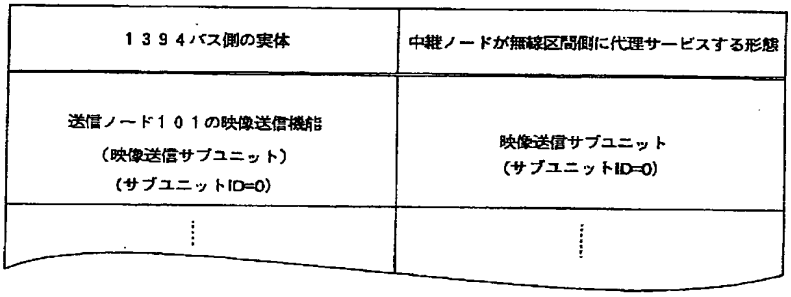
【図４３】



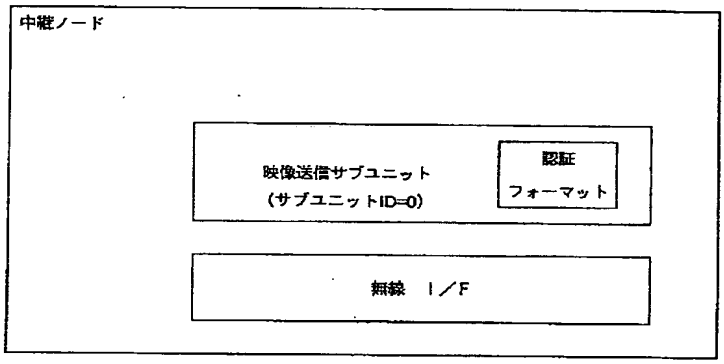
【図３４】

無線区間側の実体	中継ノードが１３９４側に代理サービスする形態
無線ノード１０３の MPEGデコード／ディスプレイ機能 (サブユニットID=0)	MPEGデコード／ディスプレイサブユニット (サブユニットID=0)
⋮	⋮

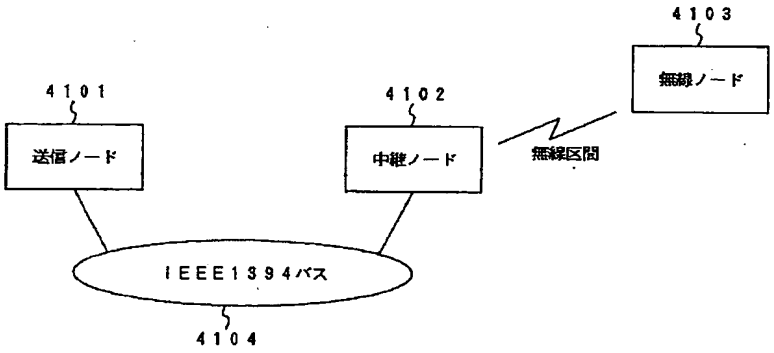
【図３５】


１３９４バス側の実体
中継ノードが無線区間側に代理サービスする形態
送信ノード１０１の映像送信機能
（映像送信サブユニット）
（サブユニットID=0）
映像送信サブユニット
（サブユニットID=0）

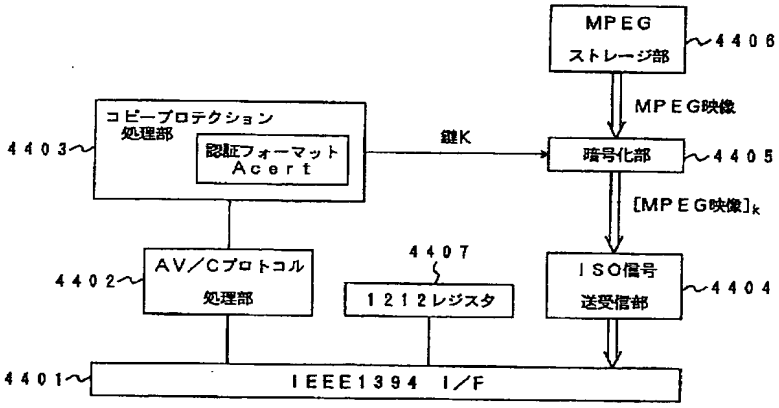
【図３７】


中継ノード
映像送信サブユニット
（サブユニットID=0）
認証
フォーマット
無線　I／F

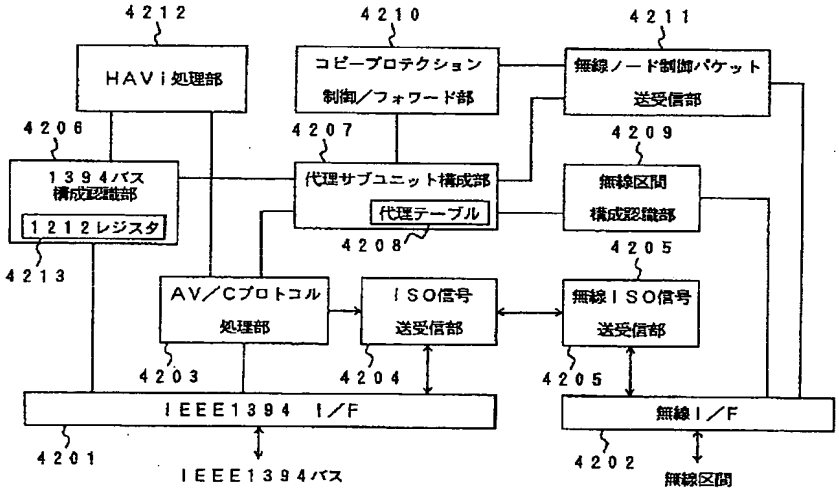
【図４０】


４１０３
無線ノード
４１０１
送信ノード
４１０２
中継ノード
無線区間
IEEE1394バス
４１０４

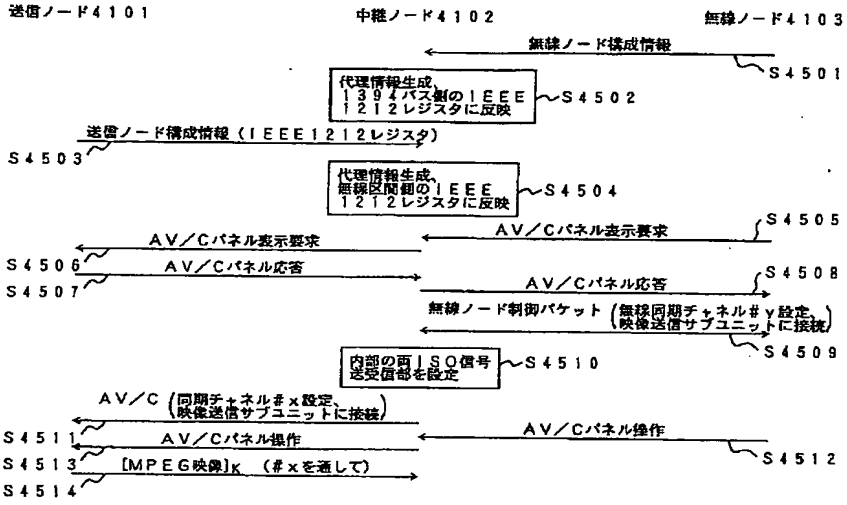
【図４１】


MPEG
ストレージ部
4406
MPEG映像
コピープロテクション
処理部
認証フォーマット
Acert
4403
鍵K
暗号化部
4405
[MPEG映像]k
4407
AV／Cプロトコル
処理部
4402
1212レジスタ
ISO信号
送受信部
4404
4401
IEEE1394 I／F

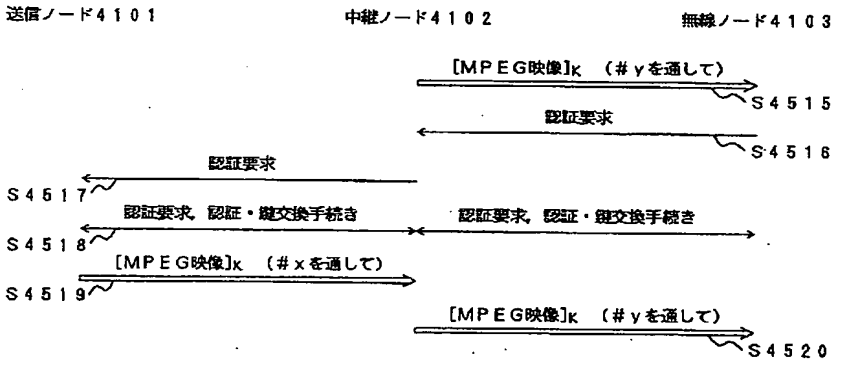
【図４２】


4212
HAVi処理部
4210
コピープロテクション
制御／フォワード部
4211
無線ノード制御パケット
送受信部
4206
1394バス
構成認識部
1212レジスタ
4213
4207
代理サブユニット構成部
代理テーブル
4208
4209
無線区間
構成認識部
4205
AV／Cプロトコル
処理部
4203
ISO信号
送受信部
4204
無線ISO信号
送受信部
4205
IEEE1394 I／F
4201
IEEE1394バス
無線I／F
4202
無線区間

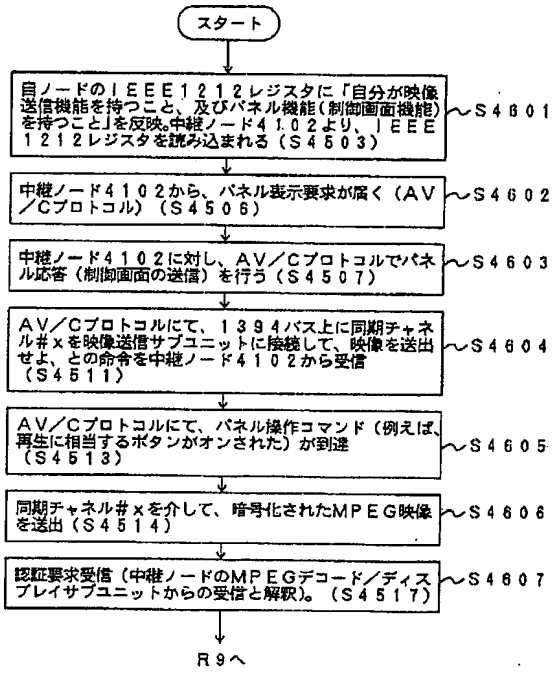
【図４４】


送信ノード４１０１
中継ノード４１０２
無線ノード４１０３
無線ノード構成情報
Ｓ４５０１
代理情報生成、
１３９４バス側のＩＥＥＥ
１２１２レジスタに反映
Ｓ４５０２
送信ノード構成情報（ＩＥＥＥ１２１２レジスタ）
Ｓ４５０３
代理情報生成、
無線区間側のＩＥＥＥ
１２１２レジスタに反映
Ｓ４５０４
Ｓ４５０５
ＡＶ／Ｃパネル表示要求
ＡＶ／Ｃパネル表示要求
Ｓ４５０６
ＡＶ／Ｃパネル応答
ＡＶ／Ｃパネル応答
Ｓ４５０８
Ｓ４５０７
無線ノード制御パケット（無線同期チャネル＃ｙ設定、映像送信サブユニットに接続）
Ｓ４５０９
内部の両ＩＳＯ信号
送受信部を設定
Ｓ４５１０
ＡＶ／Ｃ（同期チャネル＃ｘ設定、映像送信サブユニットに接続）
ＡＶ／Ｃパネル操作
Ｓ４５１１
ＡＶ／Ｃパネル操作
Ｓ４５１２
Ｓ４５１３
[ＭＰＥＧ映像]K　（＃ｘを通して）
Ｓ４５１４

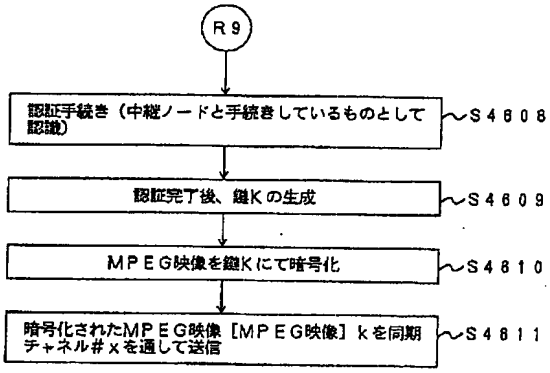
【図４５】


送信ノード４１０１
中継ノード４１０２
無線ノード４１０３
[ＭＰＥＧ映像]K　（＃ｙを通して）
Ｓ４５１５
認証要求
Ｓ４５１６
認証要求
Ｓ４５１７
認証要求，認証・鍵交換手続き
認証要求，認証・鍵交換手続き
Ｓ４５１８
[ＭＰＥＧ映像]K　（＃ｘを通して）
Ｓ４５１９
[ＭＰＥＧ映像]K　（＃ｙを通して）
Ｓ４５２０

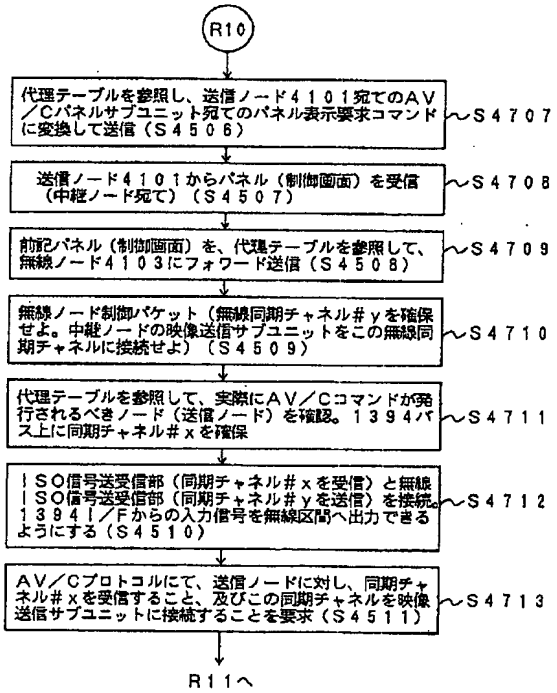
【図４６】



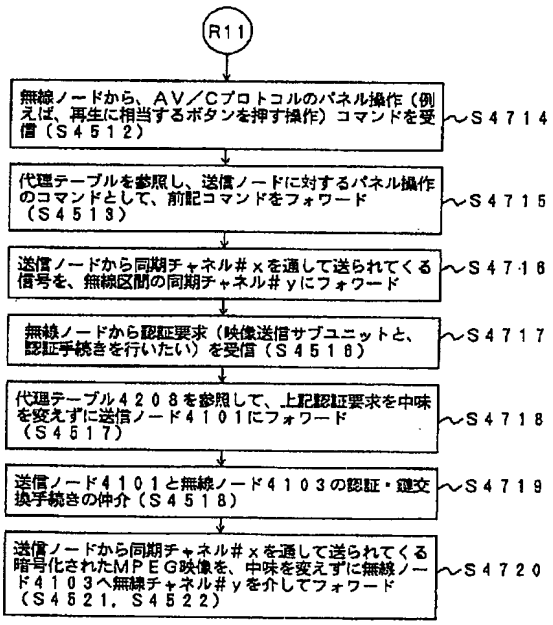
【図４７】



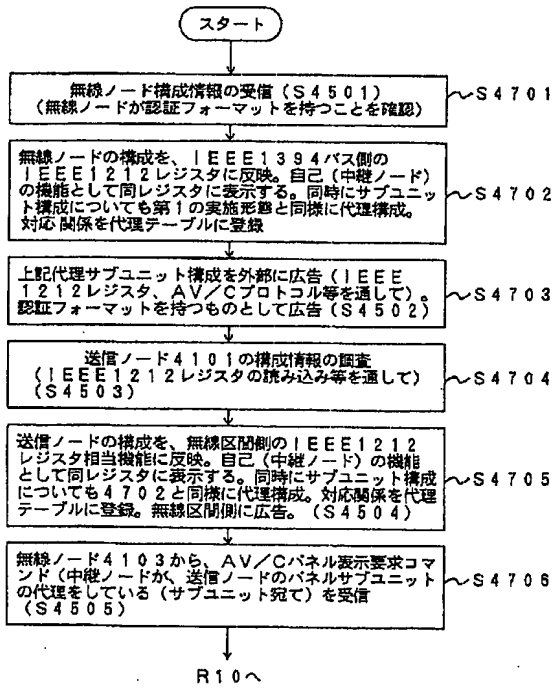
【図４９】



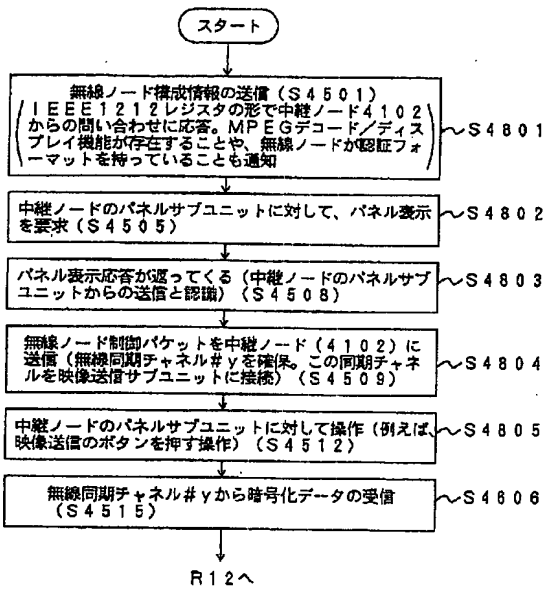
【図５０】



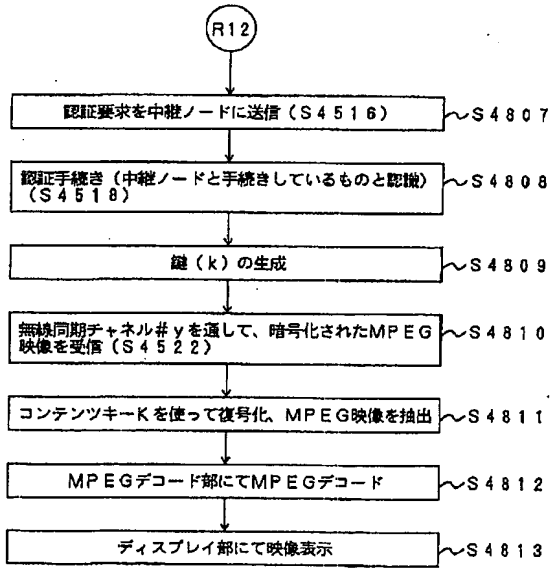
【図４８】



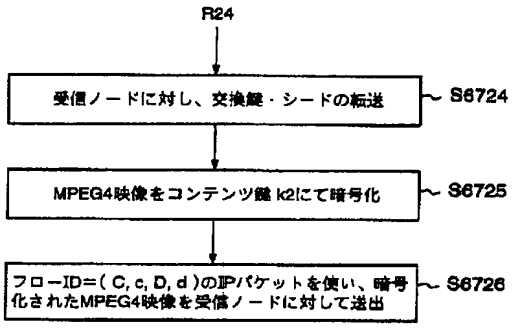
【図５１】



【図５２】



【図６９】



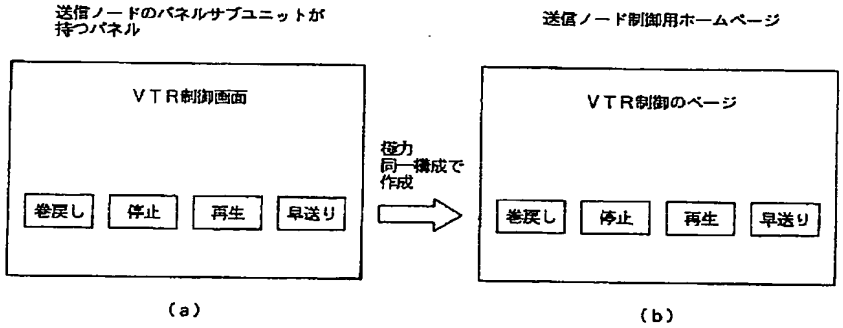
【図５３】

無線区間側の実体	中継ノードが１３９４側に代理サービスする形態
無線ノード４１０３の ＭＰＥＧデコード／ディスプレイ機能 （認証フォーマット有）	ＭＰＥＧデコード／ディスプレイサブユニット （認証フォーマット有）
無線ノード４１０３のパネル機能	パネルサブユニット
⋮	⋮

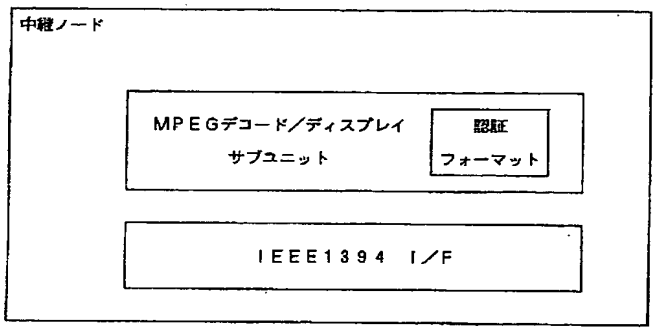
【図５４】

１３９４バス側の実体	中継ノードが無線区間側に代理サービスする形態
送信ノード４１０１の映像送信サブユニット （認証フォーマット有）	映像送信サブユニット （認証フォーマット有）
送信ノード４１０１のパネルサブユニット	パネルサブユニット
⋮	⋮

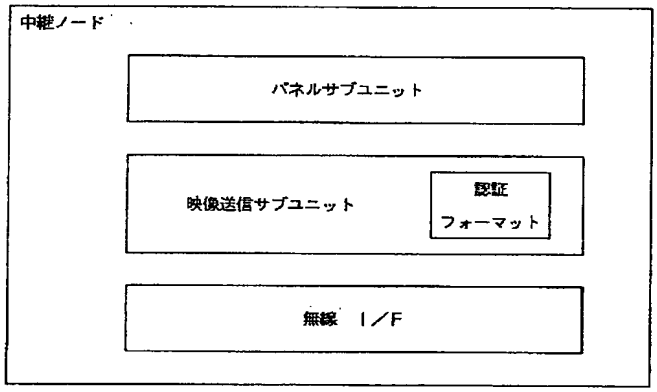
【図７２】



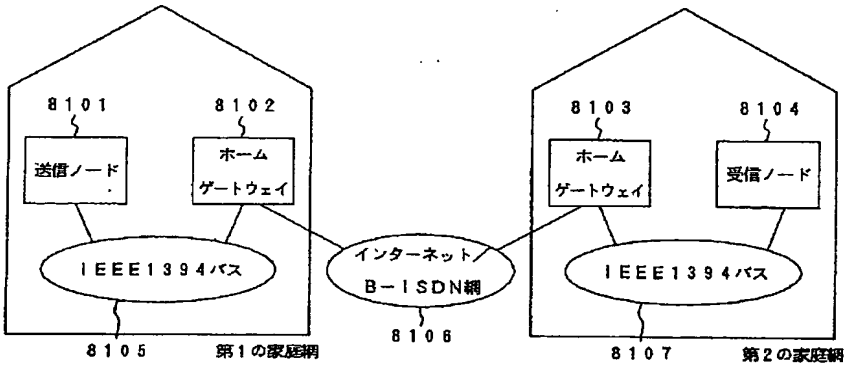
【図５５】


中継ノード
MPEGデコード／ディスプレイ
サブユニット
認証
フォーマット
IEEE1394 I／F

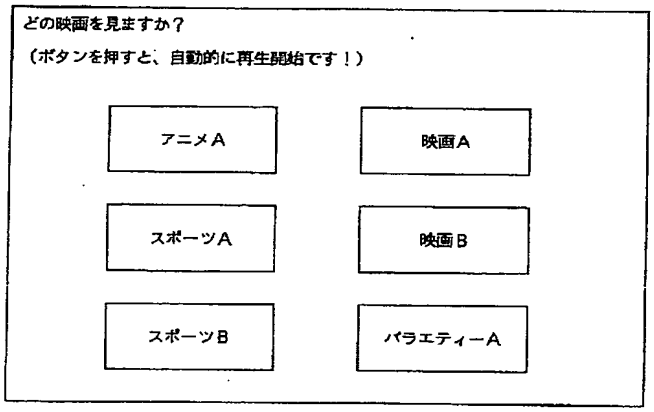
【図５６】


中継ノード
パネルサブユニット
映像送信サブユニット
認証
フォーマット
無線 I／F

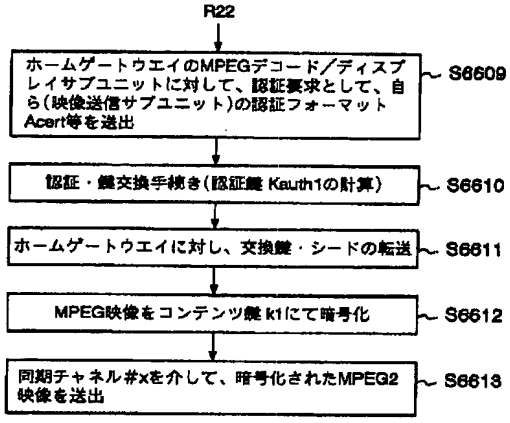
【図７３】


8101
送信ノード
8102
ホーム
ゲートウェイ
IEEE1394バス
8105
第1の家庭網
インターネット／
B－ISDN網
8106
8103
ホーム
ゲートウェイ
8104
受信ノード
IEEE1394バス
8107
第2の家庭網

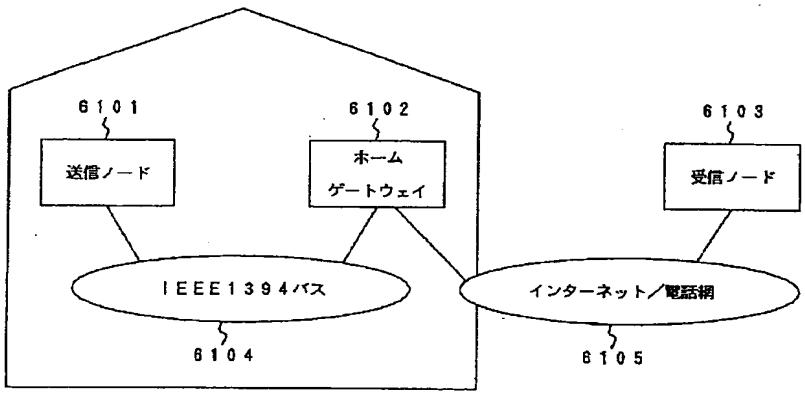
【図５７】


どの映画を見ますか？
（ボタンを押すと、自動的に再生開始です！）
アニメA
映画A
スポーツA
映画B
スポーツB
バラエティーA

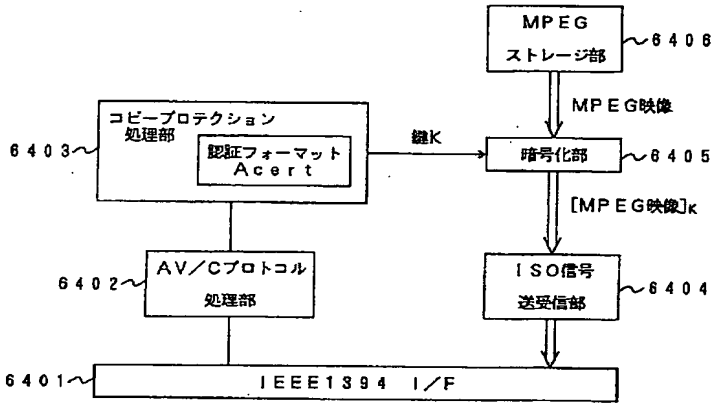
【図６５】


R22
ホームゲートウエイのMPEGデコード／ディスプレイサブユニットに対して、認証要求として、自ら(映像送信サブユニット)の認証フォーマットAcert等を送出
S6609
認証・鍵交換手続き(認証鍵 Kauth1の計算)
S6610
ホームゲートウエイに対し、交換鍵・シードの転送
S6611
MPEG映像をコンテンツ鍵 k1にて暗号化
S6612
同期チャネル#xを介して、暗号化されたMPEG2映像を送出
S6613

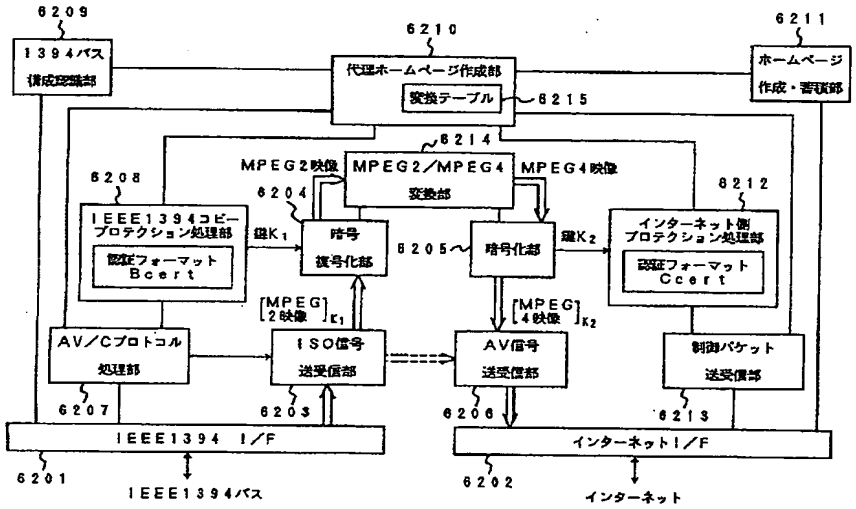
【図５８】


6101
送信ノード
6102
ホーム
ゲートウェイ
6103
受信ノード
IEEE1394バス
6104
インターネット／電話網
6105

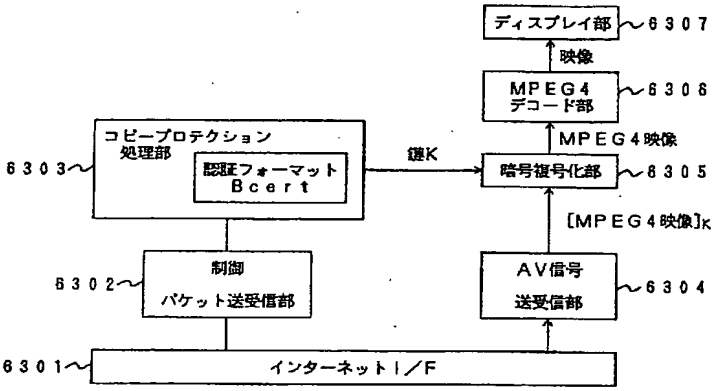
【図５９】


MPEG
ストレージ部
6406
MPEG映像
コピープロテクション
処理部
6403
認証フォーマット
Acert
鍵K
暗号化部
6405
[MPEG映像]K
AV／Cプロトコル
処理部
6402
ISO信号
送受信部
6404
6401
IEEE1394 I／F

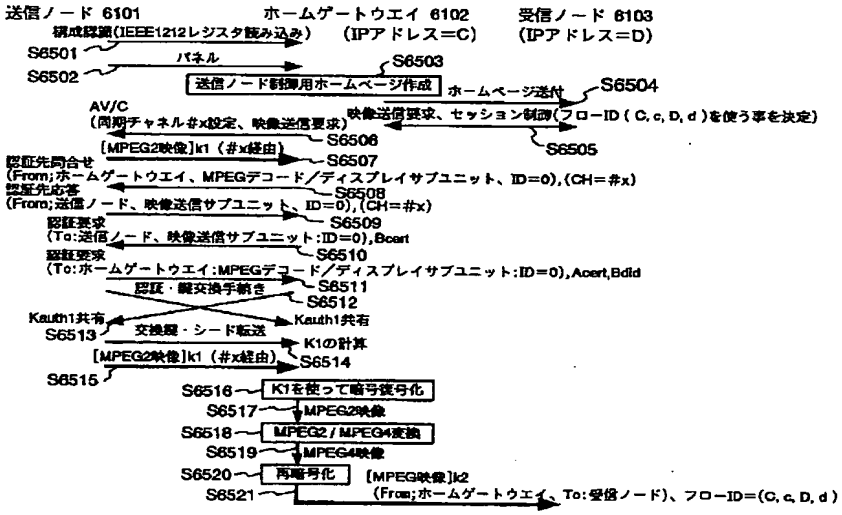
【図６０】


6209
1394バス
情報管理部
6210
代理ホームページ作成部
変換テーブル
6215
6211
ホームページ
作成・蓄積部
6214
MPEG2映像
MPEG2／MPEG4
変換部
MPEG4映像
6208
6204
6212
IEEE1394コピー
プロテクション処理部
認証フォーマット
Bcert
鍵K1
暗号
復号化部
6205
暗号化部
鍵K2
インターネット側
プロテクション処理部
認証フォーマット
Ccert
[MPEG
2映像]K1
[MPEG
4映像]K2
AV／Cプロトコル
処理部
ISO信号
送受信部
AV信号
送受信部
制御パケット
送受信部
6207
6203
6206
6213
IEEE1394 I／F
インターネットI／F
6201
6202
IEEE1394バス
インターネット

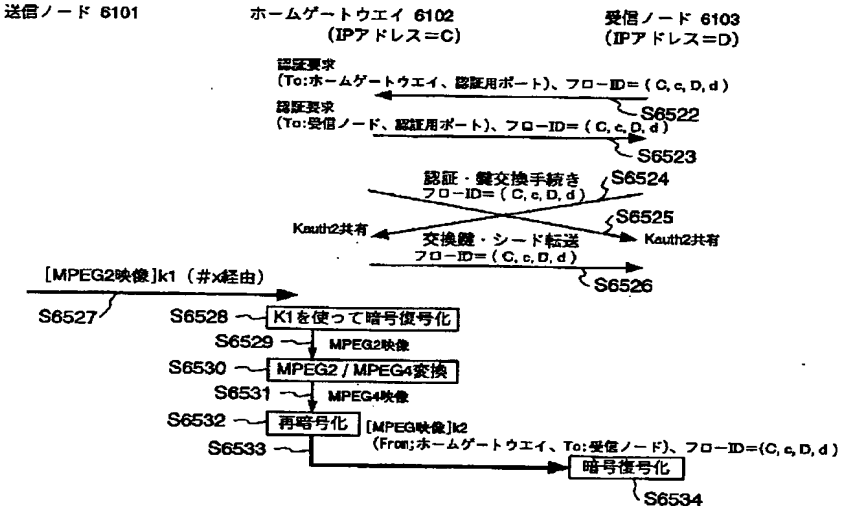
【図６１】


ディスプレイ部
6307
映像
MPEG4
デコード部
6306
MPEG4映像
コピープロテクション
処理部
認証フォーマット
Bcert
6303
鍵K
暗号復号化部
6305
[MPEG4映像]K
制御
パケット送受信部
6302
AV信号
送受信部
6304
6301
インターネットI／F

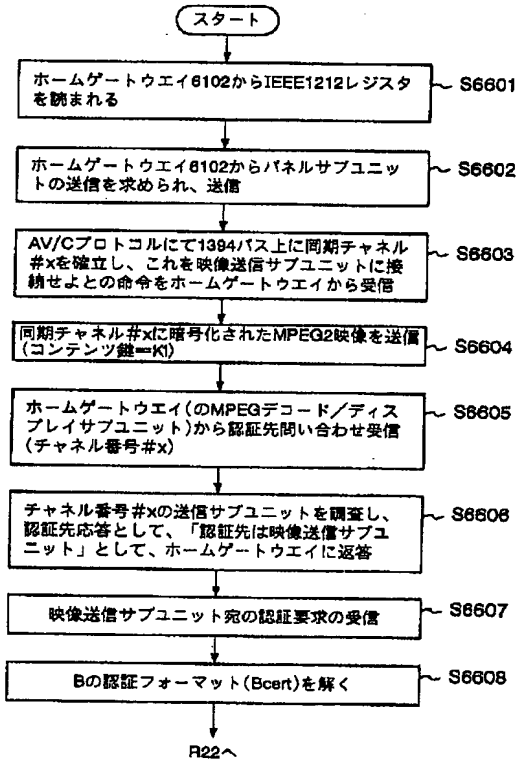
【図６２】


送信ノード 6101
ホームゲートウエイ 6102
(IPアドレス=C)
受信ノード 6103
(IPアドレス=D)
構成認識(IEEE1212レジスタ読み込み)
S6501
パネル
S6502
S6503
送信ノード制御用ホームページ作成
ホームページ送付
S6504
AV/C
(同期チャネル#x設定、映像送信要求)
映像送信要求、セッション制御(フローID(C, c, D, d)を使う事を決定)
S6506
S6505
[MPEG2映像]k1 (#x経由)
S6507
認証先問合せ
(From;ホームゲートウエイ、MPEGデコード/ディスプレイサブユニット、ID=0),(CH=#x)
S6508
認証先応答
(From;送信ノード、映像送信サブユニット、ID=0),(CH=#x)
認証要求
(To:送信ノード、映像送信サブユニット:ID=0),Bcert
S6509
認証要求
(To:ホームゲートウエイ:MPEGデコード/ディスプレイサブユニット:ID=0),Acert,BdId
S6510
認証・鍵交換手続き
S6511
S6512
Kauth1共有
Kauth1共有
S6513
交換鍵・シード転送
K1の計算
[MPEG2映像]k1 (#x経由)
S6514
S6515
S6516
K1を使って暗号復号化
S6517
MPEG2映像
S6518
MPEG2/MPEG4変換
S6519
MPEG4映像
S6520
再暗号化
[MPEG4映像]k2
S6521
(From;ホームゲートウエイ、To:受信ノード)、フローID=(C, c, D, d)

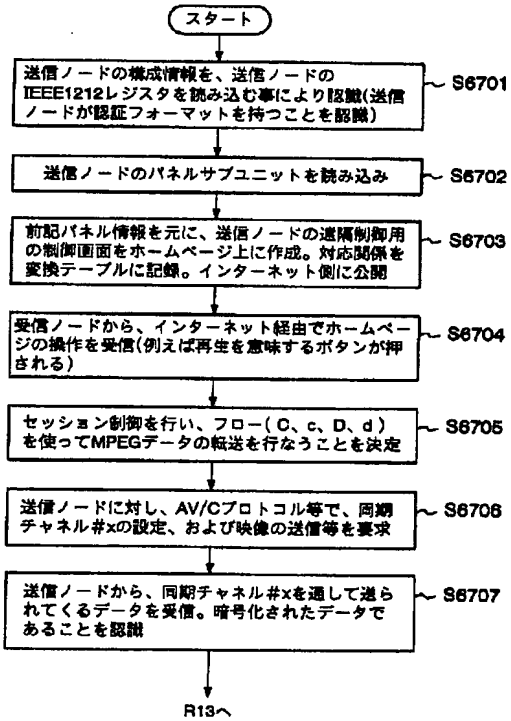
【図６３】


送信ノード 6101
ホームゲートウエイ 6102
(IPアドレス=C)
受信ノード 6103
(IPアドレス=D)
認証要求
(To:ホームゲートウエイ、認証用ポート)、フローID=(C, c, D, d)
S6522
認証要求
(To:受信ノード、認証用ポート)、フローID=(C, c, D, d)
S6523
認証・鍵交換手続き
フローID=(C, c, D, d)
S6524
S6525
Kauth2共有
交換鍵・シード転送
フローID=(C, c, D, d)
Kauth2共有
S6526
[MPEG2映像]k1 (#x経由)
S6527
S6528
K1を使って暗号復号化
S6529
MPEG2映像
S6530
MPEG2 / MPEG4変換
S6531
MPEG4映像
S6532
再暗号化
S6533
[MPEG映像]k2
(From:ホームゲートウエイ、To:受信ノード)、フローID=(C, c, D, d)
暗号復号化
S6534

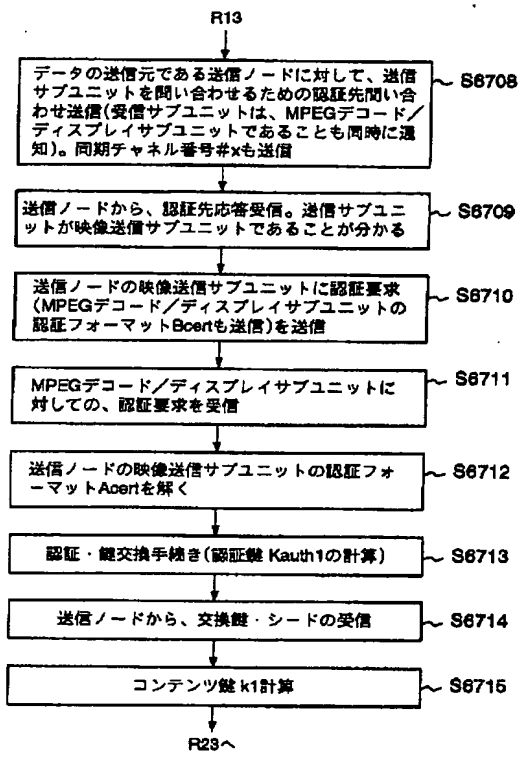
【図６４】


スタート
ホームゲートウエイ6102からIEEE1212レジスタを読まれる
S6601
ホームゲートウエイ6102からパネルサブユニットの送信を求められ、送信
S6602
AV/Cプロトコルにて1394バス上に同期チャネル#xを確立し、これを映像送信サブユニットに接続せよとの命令をホームゲートウエイから受信
S6603
同期チャネル#xに暗号化されたMPEG2映像を送信(コンテンツ鍵=K)
S6604
ホームゲートウエイ(のMPEGデコード/ディスプレイサブユニット)から認証先問い合わせ受信(チャネル番号#x)
S6605
チャネル番号#xの送信サブユニットを調査し、認証先応答として、「認証先は映像送信サブユニット」として、ホームゲートウエイに返答
S6606
映像送信サブユニット宛の認証要求の受信
S6607
Bの認証フォーマット(Bcert)を解く
S6608
R22へ

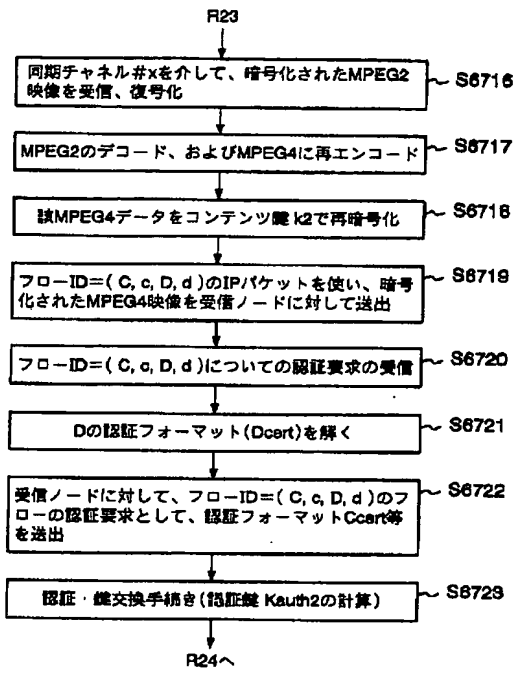
【図６６】


スタート
送信ノードの構成情報を、送信ノードのIEEE1212レジスタを読み込む事により認識(送信ノードが認証フォーマットを持つことを認識)
S6701
送信ノードのパネルサブユニットを読み込み
S6702
前記パネル情報を元に、送信ノードの遠隔制御用の制御画面をホームページ上に作成。対応関係を変換テーブルに記録。インターネット側に公開
S6703
受信ノードから、インターネット経由でホームページの操作を受信(例えば再生を意味するボタンが押される)
S6704
セッション制御を行い、フロー(C、c、D、d)を使ってMPEGデータの転送を行なうことを決定
S6705
送信ノードに対し、AV/Cプロトコル等で、同期チャネル#xの設定、および映像の送信等を要求
S6706
送信ノードから、同期チャネル#xを通して送られてくるデータを受信。暗号化されたデータであることを認識
S6707
R13へ

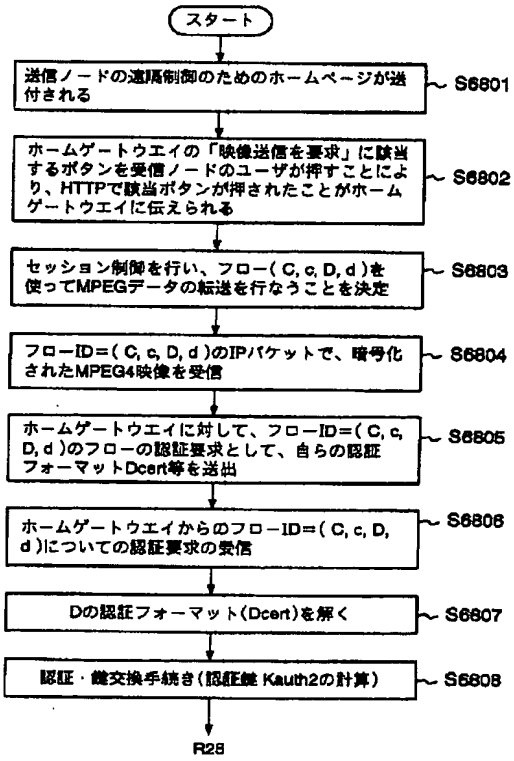
【図６７】



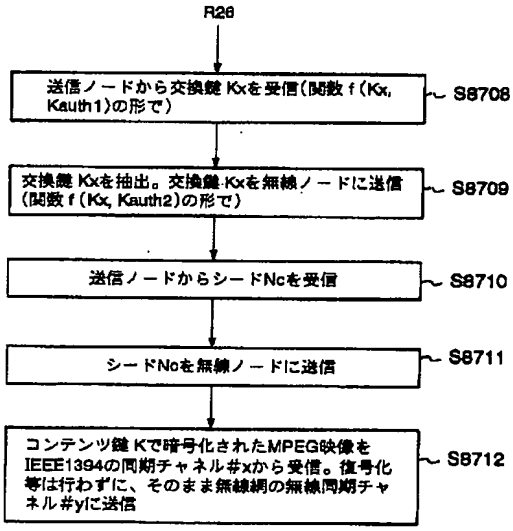
【図６８】



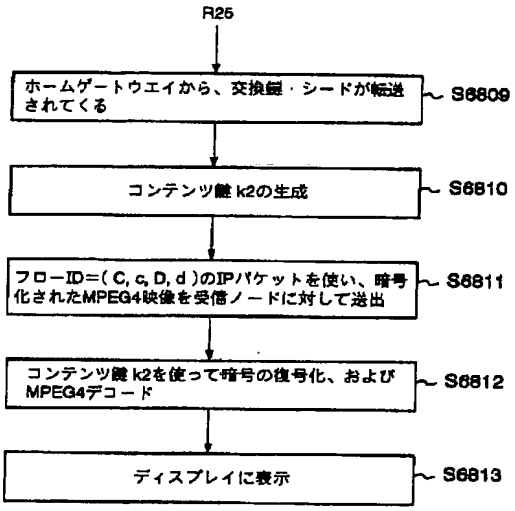
【図７０】



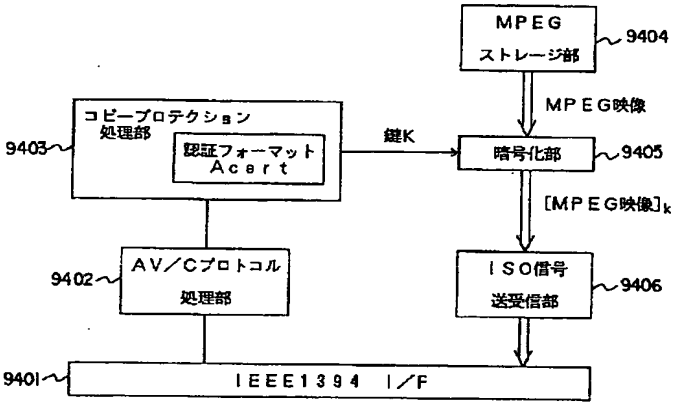
【図８４】



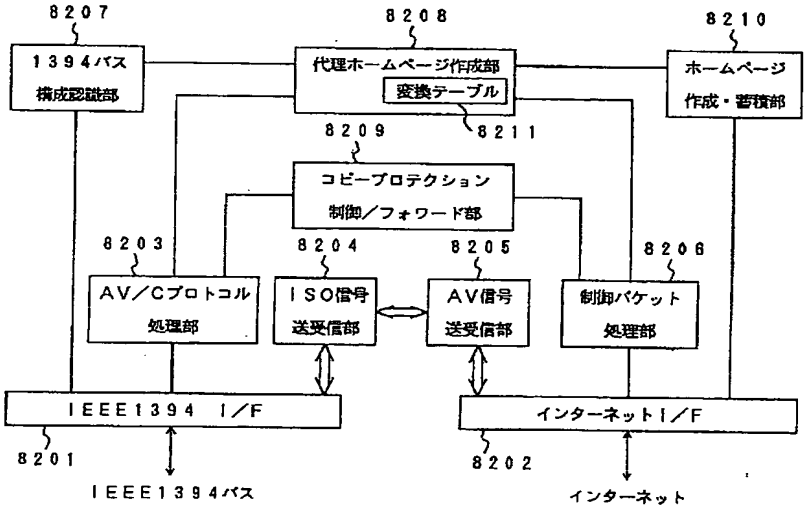
【図７１】


R25
ホームゲートウエイから、交換鍵・シードが転送されてくる
S6809
コンテンツ鍵k2の生成
S6810
フローID=(C, c, D, d)のIPパケットを使い、暗号化されたMPEG4映像を受信ノードに対して送出
S6811
コンテンツ鍵k2を使って暗号の復号化、およびMPEG4デコード
S6812
ディスプレイに表示
S6813

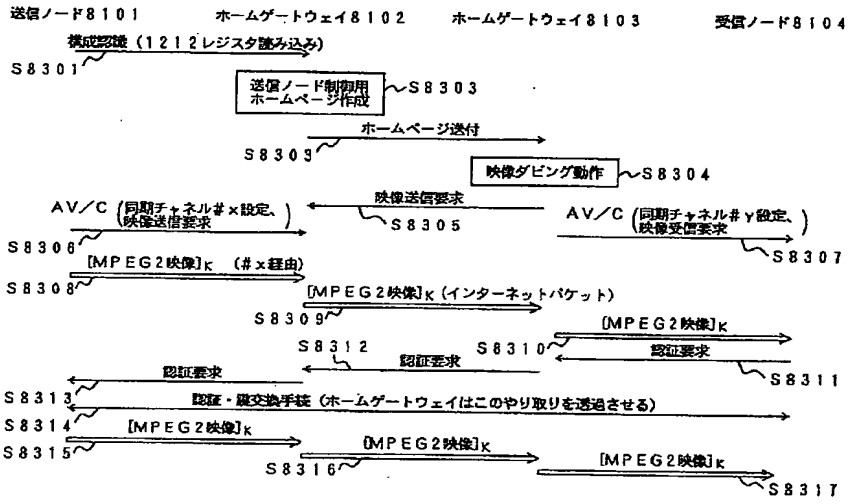
【図７８】


MPEG
ストレージ部
9404
MPEG映像
コピープロテクション
処理部
認証フォーマット
Acert
9403
鍵K
暗号化部
9405
[MPEG映像]k
AV／Cプロトコル
処理部
9402
ISO信号
送受信部
9406
IEEE1394 I／F
9401

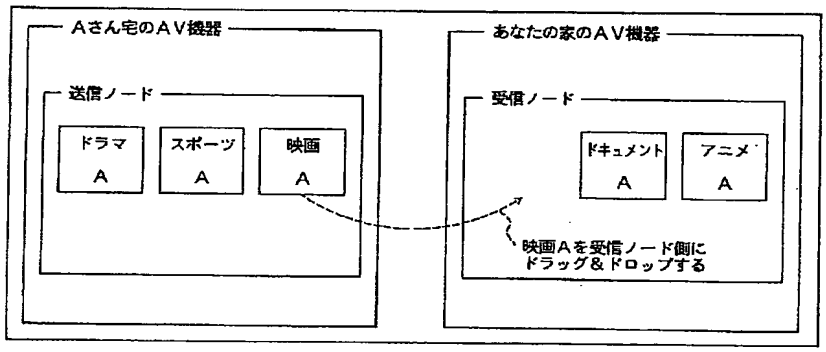
【図７４】


8207
1394バス
構成認識部
8208
代理ホームページ作成部
変換テーブル
8211
8210
ホームページ
作成・蓄積部
8209
コピープロテクション
制御／フォワード部
8203
AV／Cプロトコル
処理部
8204
ISO信号
送受信部
8205
AV信号
送受信部
8206
制御パケット
処理部
IEEE1394 I／F
8201
IEEE1394バス
インターネットI／F
8202
インターネット

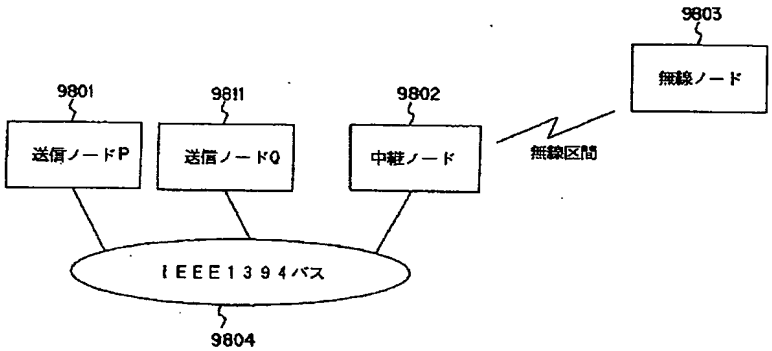
【図７５】


送信ノード８１０１
ホームゲートウェイ８１０２
ホームゲートウェイ８１０３
受信ノード８１０４
構成認識（１２１２レジスタ読み込み）
Ｓ８３０１
送信ノード制御用ホームページ作成
Ｓ８３０３
ホームページ送付
Ｓ８３０９
映像ダビング動作
Ｓ８３０４
映像送信要求
Ｓ８３０５
ＡＶ／Ｃ（同期チャネル#ｘ設定、映像送信要求）
Ｓ８３０６
ＡＶ／Ｃ（同期チャネル#ｙ設定、映像受信要求）
Ｓ８３０７
[ＭＰＥＧ２映像]Ｋ（#ｘ経由）
Ｓ８３０８
[ＭＰＥＧ２映像]Ｋ（インターネットパケット）
Ｓ８３０９
[ＭＰＥＧ２映像]Ｋ
Ｓ８３１０
認証要求
Ｓ８３１１
Ｓ８３１２
認証要求
認証要求
Ｓ８３１３
認証・鍵交換手続（ホームゲートウェイはこのやり取りを透過させる）
Ｓ８３１４
[ＭＰＥＧ２映像]Ｋ
Ｓ８３１５
[ＭＰＥＧ２映像]Ｋ
Ｓ８３１６
[ＭＰＥＧ２映像]Ｋ
Ｓ８３１７

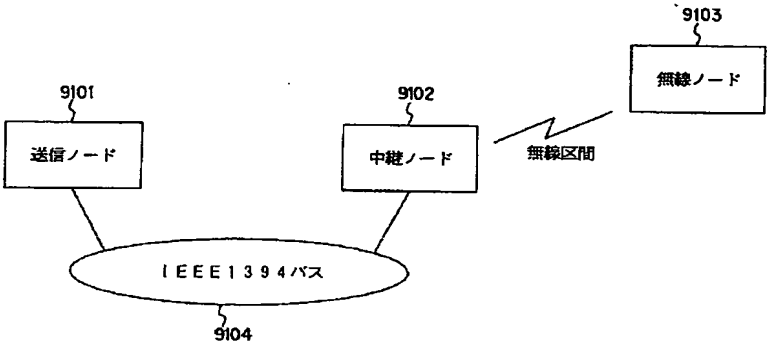
【図７６】


Ａさん宅のＡＶ機器
送信ノード
ドラマ
Ａ
スポーツ
Ａ
映画
Ａ
あなたの家のＡＶ機器
受信ノード
ドキュメント
Ａ
アニメ
Ａ
映画Ａを受信ノード側にドラッグ＆ドロップする

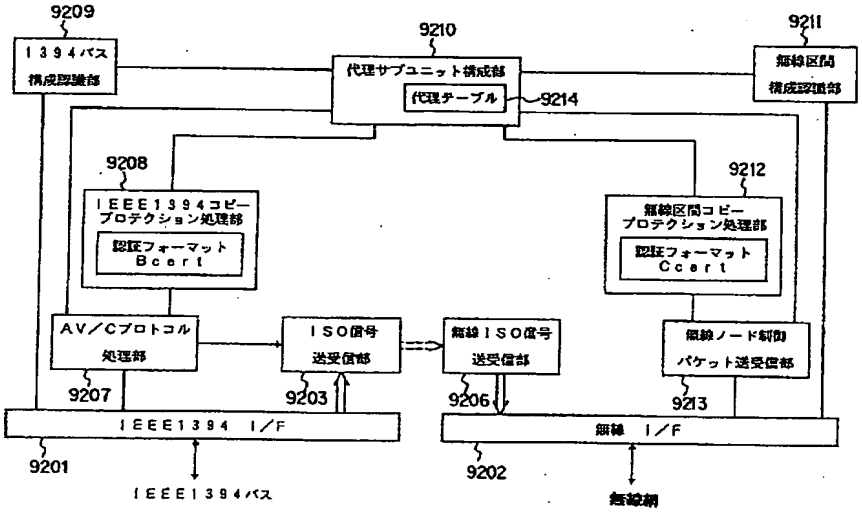
【図８７】


9803
無線ノード
9801
送信ノードP
9811
送信ノードQ
9802
中継ノード
無線区間
IEEE1394バス
9804

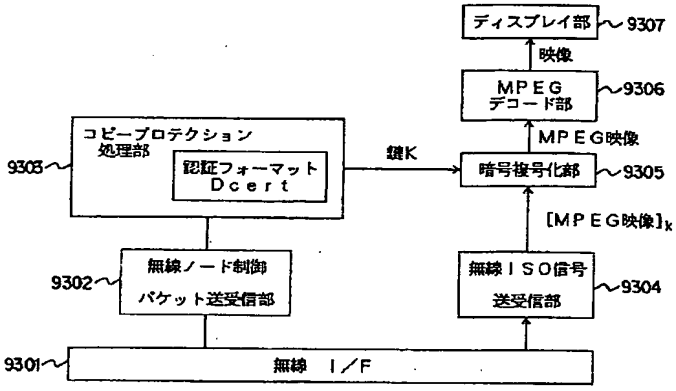
【図７７】


9103
無線ノード
9101
送信ノード
9102
中継ノード
無線区間
ＩＥＥＥ１３９４バス
9104

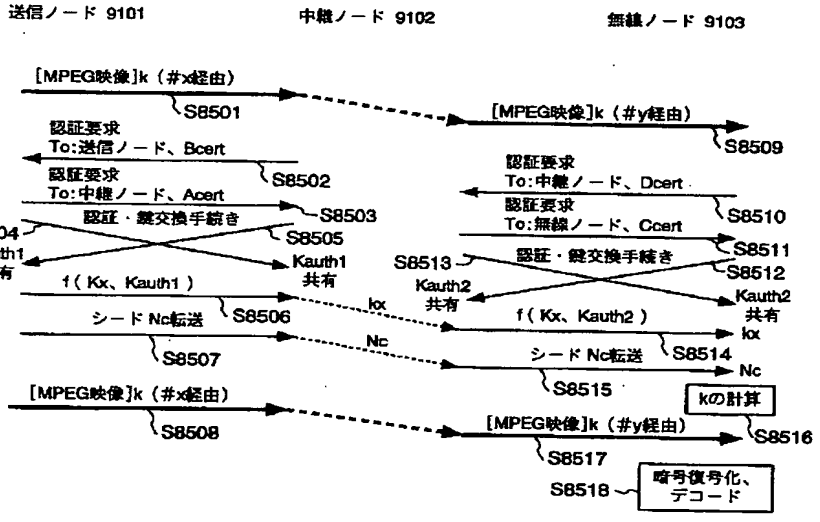
【図７９】


9209
１３９４バス
構成認識部
9210
代理サブユニット構成部
代理テーブル
9214
9211
無線区間
構成認識部
9208
ＩＥＥＥ１３９４コピー
プロテクション処理部
認証フォーマット
Ｂｃｅｒｔ
9212
無線区間コピー
プロテクション処理部
認証フォーマット
Ｃｃｅｒｔ
ＡＶ／Ｃプロトコル
処理部
ＩＳＯ信号
送受信部
無線ＩＳＯ信号
送受信部
無線ノード制御
パケット送受信部
9207
9203
9206
9213
ＩＥＥＥ１３９４　Ｉ／Ｆ
無線　Ｉ／Ｆ
9201
9202
ＩＥＥＥ１３９４バス
無線網

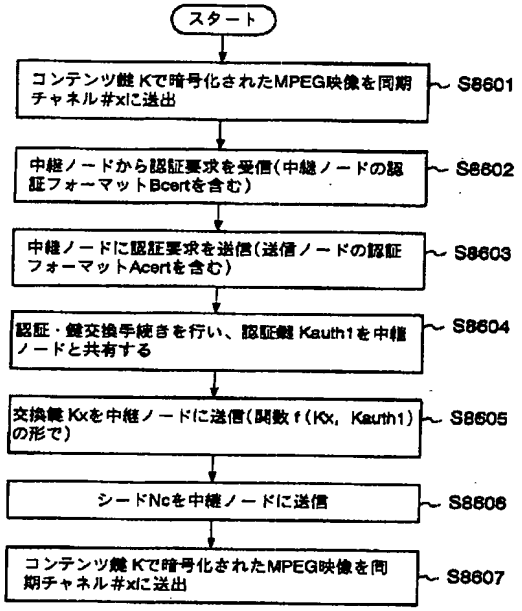
【図８０】


ディスプレイ部
9307
映像
MPEG
デコード部
9306
MPEG映像
コピープロテクション
処理部
9303
認証フォーマット
Dcert
鍵K
暗号復号化部
9305
[MPEG映像]k
9302
無線ノード制御
パケット送受信部
無線ISO信号
送受信部
9304
9301
無線 I／F

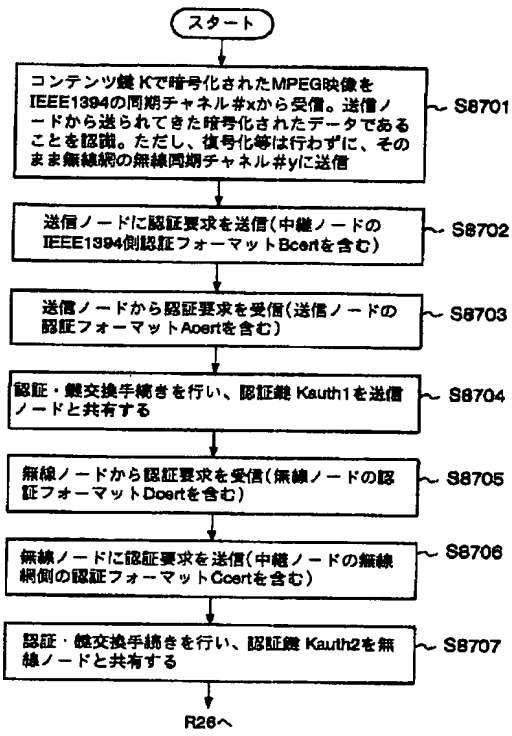
【図８１】


送信ノード 9101
中継ノード 9102
無線ノード 9103
[MPEG映像]k（#x経由）
S8501
[MPEG映像]k（#y経由）
S8509
認証要求
To:送信ノード、Bcert
S8502
認証要求
To:中継ノード、Dcert
S8510
認証要求
To:中継ノード、Acert
S8503
認証要求
To:無線ノード、Ccert
S8511
認証・鍵交換手続き
S8504
S8505
S8512
Kauth1
共有
Kauth1
共有
S8513
Kauth2
共有
Kauth2
共有
f（Kx、Kauth1）
S8506
kx
f（Kx、Kauth2）
kx
シードNc転送
S8507
Nc
シードNc転送
S8514
Nc
S8515
kの計算
[MPEG映像]k（#x経由）
S8508
[MPEG映像]k（#y経由）
S8516
S8517
S8518
暗号復号化、
デコード

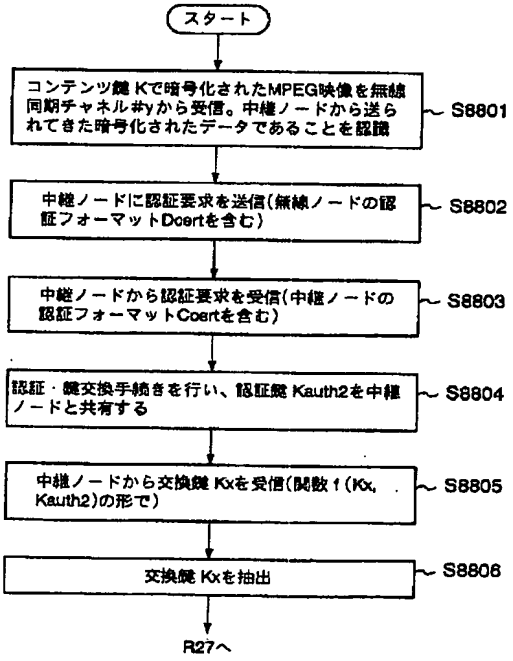
【図８２】


スタート
コンテンツ鍵 Kで暗号化されたMPEG映像を同期チャネル#xlに送出
S8601
中継ノードから認証要求を受信(中継ノードの認証フォーマットBcertを含む)
S8602
中継ノードに認証要求を送信(送信ノードの認証フォーマットAcertを含む)
S8603
認証・鍵交換手続きを行い、認証鍵 Kauth1を中継ノードと共有する
S8604
交換鍵 Kxを中継ノードに送信(関数 f(Kx, Kauth1)の形で)
S8605
シードNcを中継ノードに送信
S8606
コンテンツ鍵 Kで暗号化されたMPEG映像を同期チャネル#xlに送出
S8607

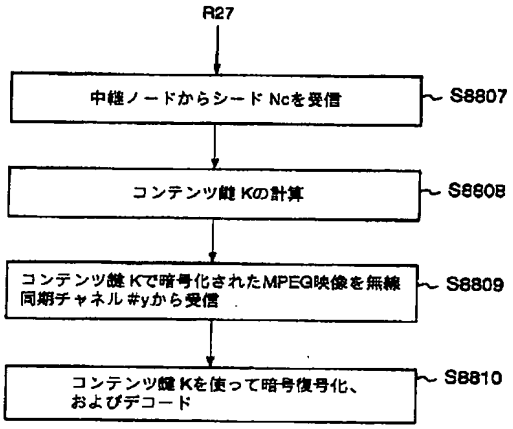
【図８３】


スタート
コンテンツ鍵 Kで暗号化されたMPEG映像をIEEE1394の同期チャネル#xから受信。送信ノードから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#yに送信
S8701
送信ノードに認証要求を送信(中継ノードのIEEE1394側認証フォーマットBcertを含む)
S8702
送信ノードから認証要求を受信(送信ノードの認証フォーマットAcertを含む)
S8703
認証・鍵交換手続きを行い、認証鍵 Kauth1を送信ノードと共有する
S8704
無線ノードから認証要求を受信(無線ノードの認証フォーマットDcertを含む)
S8705
無線ノードに認証要求を送信(中継ノードの無線網側の認証フォーマットCcertを含む)
S8706
認証・鍵交換手続きを行い、認証鍵 Kauth2を無線ノードと共有する
S8707
R26へ

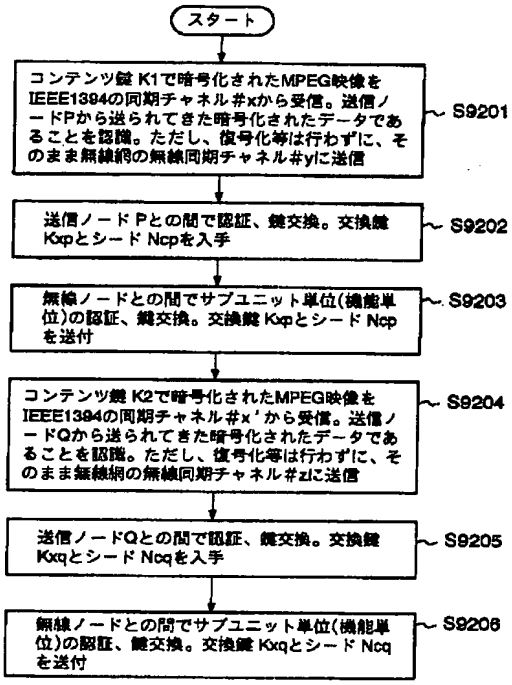
【図８５】


スタート
コンテンツ鍵 Kで暗号化されたMPEG映像を無線同期チャネル#yから受信。中継ノードから送られてきた暗号化されたデータであることを認識
S8801
中継ノードに認証要求を送信(無線ノードの認証フォーマットDcertを含む)
S8802
中継ノードから認証要求を受信(中継ノードの認証フォーマットCcertを含む)
S8803
認証・鍵交換手続きを行い、認証鍵 Kauth2を中継ノードと共有する
S8804
中継ノードから交換鍵 Kxを受信(関数 f(Kx, Kauth2)の形で)
S8805
交換鍵 Kxを抽出
S8806
R27へ

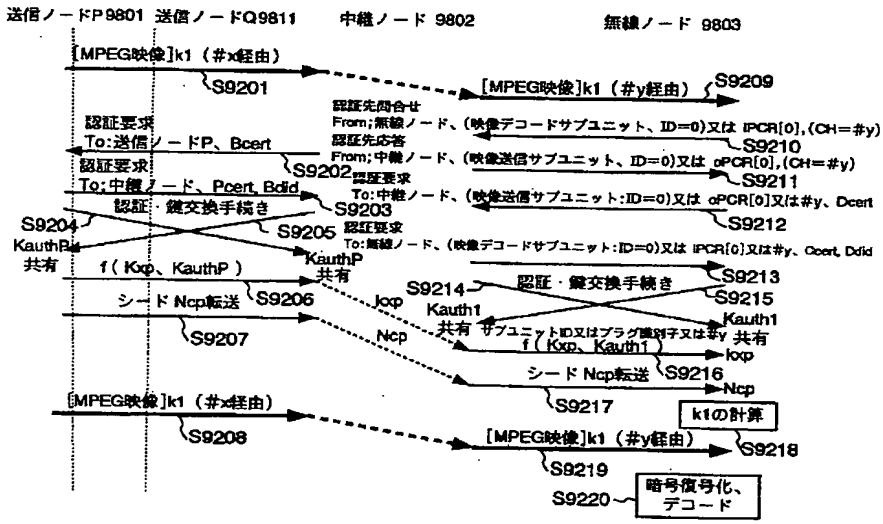
【図８６】


R27
中継ノードからシードNcを受信
S8807
コンテンツ鍵Kの計算
S8808
コンテンツ鍵Kで暗号化されたMPEG映像を無線同期チャネル#yから受信
S8809
コンテンツ鍵Kを使って暗号復号化、およびデコード
S8810

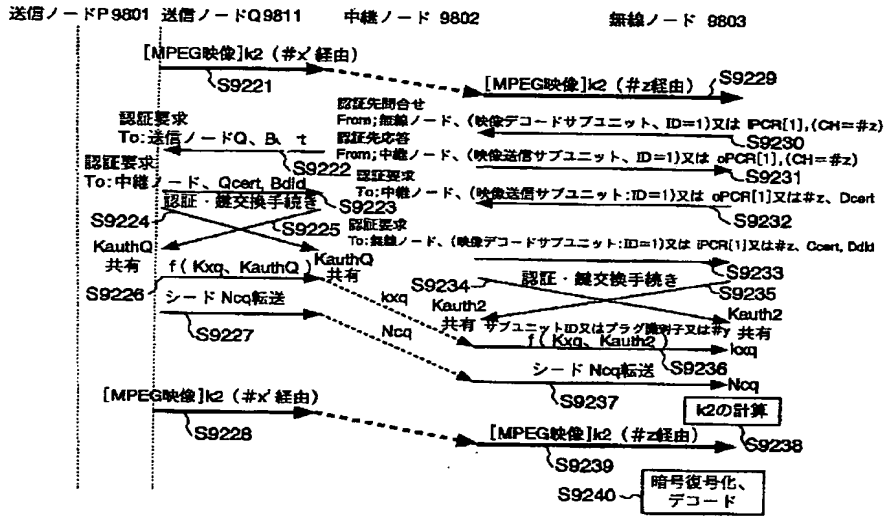
【図８８】


スタート
コンテンツ鍵K1で暗号化されたMPEG映像をIEEE1394の同期チャネル#xから受信。送信ノードPから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#yに送信
S9201
送信ノードPとの間で認証、鍵交換。交換鍵KxpとシードNcpを入手
S9202
無線ノードとの間でサブユニット単位(機能単位)の認証、鍵交換。交換鍵KxpとシードNcpを送付
S9203
コンテンツ鍵K2で暗号化されたMPEG映像をIEEE1394の同期チャネル#x'から受信。送信ノードQから送られてきた暗号化されたデータであることを認識。ただし、復号化等は行わずに、そのまま無線網の無線同期チャネル#zに送信
S9204
送信ノードQとの間で認証、鍵交換。交換鍵KxqとシードNcqを入手
S9205
無線ノードとの間でサブユニット単位(機能単位)の認証、鍵交換。交換鍵KxqとシードNcqを送付
S9206

【図８９】


送信ノードP 9801
送信ノードQ 9811
中継ノード 9802
無線ノード 9803
[MPEG映像]k1（#x経由）
S9201
[MPEG映像]k1（#y経由）
S9209
認証先問合せ
From;無線ノード、(映像デコードサブユニット、ID=0)又はIPCR[0],(CH=#y)
認証先応答
S9210
認証要求
To:送信ノードP、Bcert
S9202
From;中継ノード、(映像送信サブユニット、ID=0)又はoPCR[0],(CH=#y)
認証要求
S9211
To:中継ノード、Pcert, Bdid
認証・鍵交換手続き
S9203
To:中継ノード、(映像送信サブユニット:ID=0)又はoPCR[0]又は#y、Dcert
S9212
S9204
S9205
認証要求
KauthP
共有
To:無線ノード、(映像デコードサブユニット:ID=0)又はIPCR[0]又は#y、Ocert, Ddid
f(Kxp、KauthP)
共有
S9213
S9214
認証・鍵交換手続き
S9215
シードNcp転送
S9206
Kxp
Kauth1
Kauth1
共有
サブユニットID又はプラグ識別子又は#y
共有
S9207
Ncp
f(Kxp、Kauth1)
Kxp
シードNcp転送
S9216
Ncp
S9217
[MPEG映像]k1（#x経由）
k1の計算
S9208
[MPEG映像]k1（#y経由）
S9218
S9219
S9220
暗号復号化、デコード

【図９０】



フロントページの続き

(51)Int.Cl.⁷	識別記号	F I		テーマコード'(参考)
H04L 29/06		H04L 13/00	305Z	